НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

_____ Лапань Алекс _____
(прізвище, ім'я, по батькові)

1. Тема роботи Система захисту конфіденційної інформації в приватних організаціях _____ ,
науковий керівник роботи доцент к.т.н. Литвинова Т.В. _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «____ » 2019 р. № _____

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи _____
_____
_____

4. Зміст роботи_____
_____
_____
_____
_____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____
_____
_____
_____

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Робота обсягом 87 сторінок містить 21 ілюстрацій, 12 таблиць та 19 літературних посилань.

Метою дипломної роботи є забезпечення безпеки і достовірності передавання даних в CSaN на основі використання крипто-кодових засобів захисту інформації.

Об’єкт дослідження – процес забезпечення безпеки і достовірності передавання даних на основі використання крипто-кодових засобів захисту інформації.

Предмет дослідження – метод побудови крипто-кодових засобів захисту інформації на недвійкових рівновагових кодах.

За результатами роботи можна зробити висновок, що використання групи операцій додавання за модулем два з точністю перестановки на основі додаткової гамуючої послідовності забезпечить підвищення якості шифрування і надійності роботи, а при однократних відмовах каналів вхідної інформації – виключить можливість створення передумови витоку інформації чи зламу ключа.

Результати роботи можуть бути використані при розробці захисту конфіденційних даних в приватних організаціях.

СИСТЕМИ ЗАХИСТУ, КРИПТОСИСТЕМИ, ОЦІНКИ ЕФЕКТИВНОСТІ, КРИПТО-КОДОВІ СИСТЕМИ

ABSTRACT

The work of 87 pages contains 21 illustrations, 12 tables and 19 literary references.

The purpose of the thesis is to ensure the security and authenticity of data transfer to CSaN on the basis of the use of cryptographic code protection information.

The object of the study is the process of ensuring the security and authenticity of data transfer based on the use of cryptographic code protection information.

The subject of research is a method of constructing cryptographic code protection means for non-binary equilibrium codes.

According to the results of the work we can conclude that the use of a group of operations of addition of modules two with precision permutations on the basis of additional funchive sequence will improve the quality of encryption and reliability of work, and with single failures of incoming information channels - eliminate the possibility of creating the background of information leakage or break the key.

The results of the work can be used to develop the protection of confidential data in private organizations.

SYSTEMS OF PROTECTION, CRYPTOSYSTEMS, EVALUATION OF EFFICIENCY, CRYPTO-CODES SYSTEMS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КСіМ – комп’ютерні мережі та системи

УІР – управління інформаційними ризиками

СВА – система виявлення атак

ПЗ – програмне забезпечення

ІС – інформаційна система

ОС – операційна система

СУБД – система управління базами даних

ВСТУП

Актуальність теми. Проблема захисту комп'ютерних мереж від несанкціонованого доступу набула в останнє десятиліття особливої гостроти. Бурхливе зростання комунікаційних і обчислювальних технологій дозволяє будувати мережі розподіленої архітектури, що об'єднують велику кількість сегментів, розміщені на значній відстані одне від одного. Усе це викликає збільшення числа вузлів мереж і кількості різних ліній зв’язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі і доступу до конфіденційної інформації користувачів.

Проведені дослідження показали, що найперспективнішим напрямом в розвитку механізмів забезпечення необхідної безпеки і достовірності передавання даних є крипто-кодові системи захисту інформації, які дозволяють інтегрувати методи криптографічного перетворення і канального (завадостійкого) кодування даних, які передаються. Як випливає з результатів порівняльного аналізу, несиметричні криптоалгоритми з використанням кодових конструкцій дають змогу реалізувати криптографічний захист інформації за технологією відкритих ключів. Швидкість крипто-кодового перетворення інформації сумірна зі швидкістю шифрування (розшифрування) блоковими симетричними шифрами. Крім того практичне використання крипто-кодових засобів захисту інформації на основі інтеграції механізмів канального кодування і шифрування комплексно забезпечує безпеку і достовірність даних, які передаються.

Водночас практичне використання таких криптосистем припускає застосування методів і обчислювальних алгоритмів недвійкового рівновагового кодування. На сьогодні методи рівновагового кодування розроблено тільки на випадок двійкових кодових послідовностей, тобто науково-методичний апарат, застосовувані методи і обчислювальні алгоритми не дозволяють реалізувати

недвійкове рівновагове кодування, у тому числі і в крипто-кодових засобах захисту інформації.

Отже, актуальним науково-технічним завданням, що має важливе прикладне значення в ділянці побудови обчислювально ефективних криптографічних засобів захисту інформації, є розроблення методів і алгоритмів недвійкового рівновагового кодування і крипто-кодових засобів на їх основі для забезпечення безпеки і достовірності передавання даних у комп'ютерних системах і мережах (КСіМ).

Мета і задачі дослідження. Метою дипломної роботи є забезпечення безпеки і достовірності передавання даних в КСіМ на основі використання крипто-кодових засобів захисту інформації. Для досягнення поставленої мети необхідно вирішити такі задачі:

– проаналізувати відомі методи забезпечення безпеки і достовірності передавання даних у КСіМ та дослідити ефективність передавання даних у сучасних КСіМ і обґрунтувати вибір напряму досліджень;

– дослідити метод недвійкового рівновагового кодування на основі узагальненого біноміально–позиційного представлення чисел для крипто-кодових засобів захисту інформації в КСіМ;

– дослідити крипто-кодові засоби захисту інформації з недвійковими рівноваговими кодами для забезпечення безпеки і достовірності передавання даних у КСіМ;

– дослідити ефективність розроблених крипто-кодових засобів захисту інформації для забезпечення безпеки і достовірності передавання даних у КСіМ.

Об’єкт дослідження – процес забезпечення безпеки і достовірності передавання даних на основі використання крипто-кодових засобів захисту інформації.

Предмет дослідження – метод побудови крипто-кодових засобів захисту інформації на недвійкових рівноваговых кодах.

Методи дослідження. Основні теоретичні положення роботи отримано з використанням методів алгебраїчної теорії блокових кодів, теорії захисту

інформації, теорії кінцевих полів Галуа і теорії чисел. При дослідженні алгоритмів крипто-кодового перетворення використано елементи теорії біноміального рахунку і комбінаторики. Основні практичні результати отримано з використанням методів моделювання, теорії ймовірності і математичної статистики.

1 ОГЛЯД СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ПРИВАТНИХ ОРГАНІЗАЦІЯХ

1.1 Необхідність системи захисту конфіденційної інформації в приватних організаціях

На цей час актуальним є питання забезпечення інформаційної безпеки. В свою чергу, для забезпечення інформаційної безпеки як окремих підприємств, так і держави в цілому важливим є питання оцінки ризиків, які виникають в процесі діяльності підприємств. Для оцінки ризиків інформаційної безпеки використовуються різні методики і стандарти управління інформаційними ризиками (УІР).

Аналіз ризиків інформаційної безпеки є методом виявлення вразливостей і загроз, оцінки можливого впливу, що дозволяє вибирати адекватні захисні заходи для тих систем і процесів, у яких вони необхідні. Методики аналізу інформаційних ризиків дозволяють забезпечити ефективний і актуальний захист інформаційного простору підприємств і можливість вчасно реагувати на загрози інформаційній безпеці.

В цілому аналіз ризиків інформаційної безпеки передбачає облік активів і встановлення їхньої цінності для підприємства, класифікацію загроз і вразливостей, визначення ймовірності й впливу на діяльність підприємства цих потенційних загроз, а також оптимізацію витрат між збитками від впливу загроз і вартістю захисних заходів. Активи бувають матеріальні (мережеве обладнання, комп'ютери, програмне забезпечення, устаткування, матеріали) і нематеріальні (репутація, інформація, авторське право). Кількісно оцінити вартість нематеріальних активів набагато важче, ніж матеріальних.

Оцінка активів може проводитися кількісними та якісними методами. Фактична вартість активів визначається на підставі вартості їх придбання,

розробки й підтримки. Цінність активів визначається мірою їх необхідності для уповноважених і неуповноважених користувачів і власників.

Для забезпечення ефективності аналізу ризиків інформаційної безпеки на підприємстві має бути створена група управління інформаційними ризиками. До складу цієї групи входять керівники підрозділів, IT-працівники, розроблювачі додатків. Одним з перших завдань УІР-групи є визначення вартості активів підприємства і формування звіту з цих питань. Керівництво підприємства, проаналізувавши цей звіт, визначає обсяг УІР-проекту.

При визначенні вартості активів УІР-група повинна враховувати корисність і значення активів для підприємства; цінність активів для конкурентів, користувачів і власників цих активів; витрати на купівлю, розроблення, захист, заміну або ремонт активів при їх виході з ладу або втраті; наслідки у випадку компрометації активів тощо. Саме цінність активів визначає механізми безпеки та захисні заходи для їх захисту.

Після визначення цінності активів, відбувається ідентифікація загроз інформаційній безпеці підприємства, яка дозволяє встановити найбільш вразливі місця. Під час цієї ідентифікації встановлюються джерела загроз та їх наслідки, після чого проводиться аналіз можливих вразливостей від цих загроз і окреслюються шляхи протидії загрозам. Наприклад, джерелом загроз може бути хакер, який одержує доступ до конфіденційної інформації, за рахунок вразливості у вигляді великої кількості служб, запущених на сервері підприємства.

Після виявлення вразливостей і пов'язаних з ними загроз УІР-група повинна проаналізувати ризики потенційного збитку, а саме несанкціоноване розголошення конфіденційної інформації, зниження продуктивності роботи, пошкодження інформації або інформаційних систем та інші і доповісти про це керівництву підприємства для вживання адекватних заходів протидії.

Проведемо порівняльний аналіз найбільш поширених на цей час методик оцінки ризиків інформаційної безпеки.

Методикою оцінки ризиків OCTAVE займається американський інститут Software Engineering Institute [1]. Ця методологія передбачає здійснення процесу аналізу ризиків інформаційної безпеки лише працівниками підприємства без залучення зовнішніх консультантів, через те що такі працівники краще розуміють потреби підприємства і властиві йому ризики.

За цією методикою відбувається розробка профілю загроз, встановлення вразливостей інформаційній безпеці і розроблення стратегії забезпечення безпеки. Для кожного джерела загроз будується дерево варіантів, яке наочно показує вигляд загрози і шляхи її усунення. При оцінці ризиків інформаційній безпеці формується шкала за трьома позиціями: високий, середній та низький рівень ризику і встановлюється можливий фінансовий збиток. Основною перевагою даної методики є загальнодоступність і безкоштовність.

Для проведення якісної оцінки ризиків використовується груповий процес аналізу ризиків FRAP. Ця методика побудована таким чином [2], що будь-яка людина з навиками організації групової роботи зможе успішно провести аналіз ризиків інформаційної безпеки. Згідно з цією методикою необхідно здійснити такі етапи, як мозкова атака для встановлення всіх загроз інформаційній безпеці підприємства; визначення ймовірності та вразливостей для кожної загрози за шкалою велика/середня/низька; формування звіту за результатами можливого впливу кожної із загроз. Перевагою цієї методики є швидкість і простота прийняття рішень.

Також заслуговує на увагу метод аналізу й керування ризиками Центрального агентства по комп'ютерах і телекомунікаціях (ССТА) Великобританії CRAMM. Цей метод поєднує кількісні та якісні методики оцінки ризиків. Метод є універсальним і може використовуватися великими і малими, державними і комерційними підприємствами.

Версії програмного забезпечення CRAMM орієнтовані на різні типи підприємств і відрізняються своїми базами знань [3]. Для комерційних підприємств існує комерційний профіль, а для державних - урядовий профіль.

Урядовий профіль дозволяє проводити аудит на відповідність вимогам стандарту ITSEC.

Метод CRAMM дозволяє економічно обгрунтувати витрати підприємства на забезпечення інформаційної безпеки і безперервність бізнесу. Він розділений на три сегменти: ідентифікація й оцінка активів, аналіз загроз і вразливостей, вибір контрзаходів. Цей метод, назважаючи на значну універсальність та функціональність, має такі недоліки як необхідність спеціальної підготовки користувачів і значна вартість ліцензії.

Для оцінки ризиків інформаційної безпеки існують інші методики, які подібні до проаналізованих.

З проведеного аналізу можна навести такі рекомендації по вибору методик оцінки ризиків інформаційної безпеки: для невеликих підприємств доцільно використовувати методику OCTAVE, для середніх – FRAP, а для великих – CRAMM.

На сьогодні розвиток комп’ютерних мереж впливає на більшість сфер економічної діяльності. Значна кількість підприємств та організацій по всьому світу використовують комп’ютерні мережі для керування виробничими процесами і персоналом, розподілу ресурсів та підключення віддалених користувачів до мережі Internet. Це дає їм ряд очевидних переваг - прискорення виробничих процесів, підвищення мобільності і оперативності доступу до інформації та послуг, можливість віддаленого управління банківськими рахунками, замовлення і оплати товарів і послуг. Це зумовило зна- чне зростання вартості інформації, циркулюючої в комп’ютерних мережах.

Забезпечення працездатності мереж, а також працездатності функціонуючих в них інформаційних систем, залежить не тільки від надійності використовуваної апаратури, але і від здатності мережі протистояти цілеспрямованим діям, які спрямовані на порушення її роботи.

Слід зазначити, що атаки на інформаційні системи з кожним роком стають усе досконалішими, масштабнішими та інтенсивнішими. Тому актуальною є проблема розробки та вдосконалення систем виявлення вторгнень, головним

завданням яких є саме виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі. Постійний стрімкий розвиток методів та способів деструктивного програмного впливу на інформаційні системи зумовлює необхідність проведення порівняльного аналізу типів систем виявлення атак та запобігання вторгненням з метою визначення найбільш ефективних механізмів захисту інформації.

Системи аналізу захищеності

Системи аналізу захищеності досліджують налаштування елементів захисту операційних систем робочих станцій і серверів, аналізують топологію мережі, шукають незахищені мережеві з'єднання, досліджують налаштування міжмережевих екранів. Дані системи дозволяють значно знизити ризик наявності невиявлених загроз у системі захисту мереж.

До сучасних засобів моніторингу комп'ютерних атак відносяться аналізатори трафіку, такі як "сніфери" і системи виявлення атак.

Істотним недоліком даних систем є те, що аналіз трафіку адміністратором безпеки здійснюється практично вручну із застосуванням лише найпростіших засобів автоматизації, таких як аналіз протоколів. У зв'язку з цим дані системи не підходять для моніторингу великих обсягів трафіку мереж масштабу міста.

Рішенням цієї проблеми є застосування засобів моніторингу, здатних аналізувати трафік великого об'єму в режимі реального часу. До таких засобів моніторингу відносяться системи виявлення атак.

Системи виявлення атак (СВА) являють собою окремий клас програмних засобів (ПЗ), під яким розуміють програми, процедури, правила, а також, якщо передбачено, супутніх їм документації та даних, що відносяться до функціонування системи обробки інформації. Повна назва СВА – це системи виявлення і запобігання атак, так як саме в можливості автоматизованої протидії атакам полягає одна з основних переваг таких систем, у порівнянні, наприклад, із засобами, заснованими на людському факторі. Проте надалі буде використовуватися найбільш усталена назва - система виявлення атак.

Використання СВА дозволяє вирішити цілий ряд завдань, що забезпечують досягнення цілей інформаційної безпеки:

- розпізнавання відомих і, по можливості, невідомих атак та по- передження персоналу, що відповідає за забезпечення інформаційної безпеки (ІБ);
- статистичний аналіз шаблонів аномальних дій;
- моніторинг і аналіз користувацької, мережевої та системної активності;
- контроль цілісності файлів та інших ресурсів інформаційної системи (ІС);
- аудит системної конфігурації і виявлення вразливостей;
- інсталяція і підтримка роботи серверів-пасток для запису інформації про порушників;
- зниження навантаження на персонал (або звільнення від нього), що відповідає за ІБ, від поточних рутинних операцій з контролю за користувачами, системами і мережами, які є компонентами ІС;
- надання можливості управління функціями захисту не спеціалістам в області інформаційної безпеки.

Сучасні технології виявлення атак

Під виявленням атак розуміють процес оцінки подій ІС та її інформаційних потоків, який реалізується за допомогою аналізу журналів реєстрації операційних систем (ОС) і додатків або мережевого трафіку. Реалізація більшості мережевих атак здійснюються в три етапи.

Перший, підготовчий, етап полягає в пошуку передумов для здійснення тієї чи іншої атаки. На даному етапі шукають вразливості, використання яких робить можливим в принципі реалізацію атаки, яка і складає другий етап. На третьому етапі атака завершується. При цьому перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук порушником вразливостей за допомогою сканерів безпеки вже вважається атакою.

Технології виявлення атак постійно розвиваються і удосконалюються, і ця область постійно залучає нових виробників і розробників. Незважаючи на брак

теоретичних основ технології виявлення атак, існують досить ефективні методи, що використовують на сьогодні.

Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках. Тип слід визначати, виходячи з таких характеристик:

Спосіб контролю за системою. За способами контролю за системою поділяються на network-based, host-based і application- based.

Спосіб аналізу. Це частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації, і приймає рішення, чи відбувається проникнення. Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection).

Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

Більшість комерційних систем виявлення атак є real-time network-based системами.

Виявлення атак вимагає виконання однієї з двох умов: або знання всіх можливих атак та їх модифікацій, чи розуміння очікуваної поведінки контрольованого об’єкта системи. Всі існуючі технології виявлення мережевих атак можна розділити на два типи: методи на основі сигнатур (зразків і правил); методи на основі аномалій.

Зазвичай в СВА намагаються поєднувати обидві технології, щоб усунути недоліки, властиві кожній окремо. Перевага “аномальних” систем - виявлення невідомих або нових видів атак, які можуть “обійти” СВА. Реєстрація такого роду подій тягне за собою їх аналіз адміністратором, створення для них шаблону і внесення останнього до бази даних СВА. Системи, засновані на методі аномалій, вважаються досить перспективними, але ще розвиваються і перебувають у стадії дослідження.

Особливістю технології виявлення атак на основі сигнатур є процес опису атаки у вигляді шаблону або сигнатури і пошуку даного шаблону в

контрольованому просторі (наприклад, мережевому трафіку або журналі реєстрації). Така СВА може виявити всі відомі атаки, але вона мало пристосована для виявлення нових, ще невідомих, атак.

При розробці СВА, заснованих на цьому підході, виникають дві основні проблеми. Перша полягає у створенні механізму опису сигнатур, тобто мови опису атак, а друга проблема виражається в наступному: як записати атаку, щоб зафіксувати всі можливі її модифікації? Схема технології виявлення атак на основі сигнатур показана на рисунку 1.1.

Переваги:

- Детектори зловживань ефективно визначають атаки і дуже рідко створюють помилкові повідомлення;
- Детектори зловживань швидко й надійно діагностують використання конкретного інструментального засобу або технології атаки. Це дає змогу адміністратору скоригувати заходи для забезпечення безпеки;
- Швидкість аналізу.

Недоліки:

- Оскільки детектори зловживань виявляють лише відомі їм атаки, слід постійно оновлювати їхні бази даних для отримання сигнатур нових атак;
- Більшість детекторів зловживань розроблено так, що вони ви- користовують лише певні сигнатури, а це не дає виявити мо- жливі варіанти атак;

Технологія виявлення атак на основі аномалій побудована на припущенні, що аномальна поведінка суб'єкта ІС (системи, програми, користувача), тобто, як правило, атака або яка-небудь ворожа дія часто проявляється як відхилення від нормальної поведінки. Зазвичай системи виявлення аномальної активності використовують як джерело даних журнали реєстрації і поточна діяльність користувача, хоча існують приклади системи виявлення аномалій в мережевому трафіку.

Традиційне використання цієї технології полягає не в чіткому виявленні атак, а у визначенні підозрілої активності, що відрізняється від нормальної.

Основна проблема методу полягає в тому, щоб визначити критерій нормальної активності. Необхідно також встановити допустимі відхилення від нормального трафіку, які ще не вважатимуться атакою.

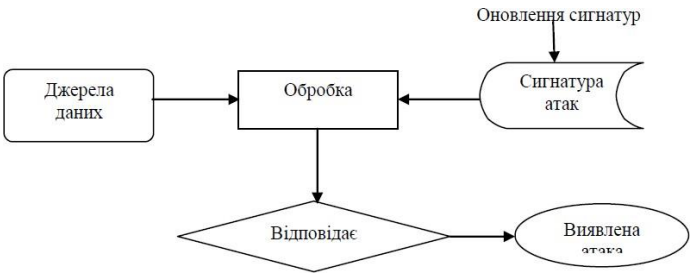


Рисунок 1.1 – Схема виявлення атак на основі сигнатур

При використанні даної технології виявлення атак можливі два варіанти неправильного виявлення атаки:

- виявлення дії, яка не є атакою, і віднесення його до класу атак;
- пропуск атаки, яка не підпадає під сигнатури атак. Цей випадок більш небезпечний, ніж помилкове віднесення дозволеного дії до класу атак. Підкатегорією такого методу є аналіз на основі профілів, коли нормальна поведінка визначається для окремих суб'єктів (користувачів / систем).

Іноді елементи такого аналізу зустрічаються і в інших методах, скажімо, в розшифровці протоколу, коли виявлений елемент, що не належить наперед визначеному протоколу або порушує правила використання протоколів.

Схема типової системи виявлення аномалій показана на рисунку 1.2.

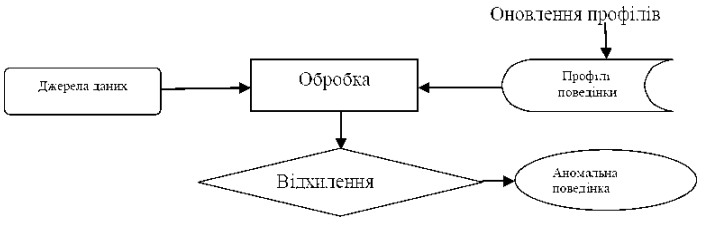


Рисунок 1.2 – Схема системи виявлення аномальної поведінки

Прикладами аномальної поведінки є велика кількість з’єднаньза короткий проміжок часу, високі завантаження центрального процесора і коефіцієнт мережевого навантаження або використання периферійних пристроїв, які зазвичай не використовуються.

Якщо описати профіль нормальної поведінки суб’єкта, то будь-яке відхилення від нього можна охарактеризувати як аномальна поведінка.

Переваги:

СВА, що виявляють аномалії, фіксуючи несподівану поведінку системи, отримують можливість визначати симптоми атак, не маючи відомостей про їхні конкретні деталі;

Детектори аномалій збирають інформацію, якою в подальшому можуть скористатися детектори зловживань для визначення сигнатур.

Недоліки:

Під час виявлення аномалій, як правило, створюється велика кількість помилкових сигналів про атаки у разі непередбачуваної поведінки користувачів і мережної активності;

Цей метод часто потребує певного етапу навчання системи, під час якого визначаються характеристики нормальної поведінки. Якість проведення цього навчання суттєво впливає на подальшу ефективність СВА;

Не можна реалізувати опис атаки за елементами. Повідомляється те, що відбувається щось підозріле;

Дана технологія значно залежить від середовища функціонування як визначального фактор анормальної поведінки;

- Відносно низька швидкість аналізу;
- Трудомістке завдання побудови профілів суб’єктів ІС.

1.2 Оцінка ймовірних загроз конфіденційній інформації організації

Для забезпечення інформаційної безпеки як окремих підприємств, так і держави в цілому важливим є питання оцінки ризиків, які виникають в процесі діяльності підприємств. Для оцінки ризиків інформаційної безпеки використовуються різні методики і стандарти управління інформаційними ризиками.

Аналіз ризиків інформаційної безпеки є методом виявлення вразливостей і загроз, оцінки можливого їх впливу, що дозволяє вибирати адекватні захисні заходи для тих систем і процесів, у яких вони необхідні. Методики аналізу інформаційних ризиків дають змогу забезпечити ефективний і актуальний захист інформаційного простору підприємств і можливість вчасно реагувати на загрози інформаційній безпеці.

Аналіз методик оцінки ризиків інформаційної безпеки

Ризик є невід'ємним атрибутом фінансово-господарської діяльності підприємств і потребує значної уваги з боку фінансових менеджерів. Існування певного рівня ризику операцій зовсім не означає, що від них треба відмовитися. Адже, відмова буде рівнозначною втраті очікуваних доходів і прибутків. В усьому потрібна міра і виваженість фінансових рішень.

Важлива роль у визначенні допустимого рівня ризику, прогнозуванні ймовірності настання ризикових подій та своєчасній нейтралізації їх негативних наслідків відводиться ризик-менеджменту.

Для функціонування ризик-менеджменту повинен існувати орган управління ризиками з певними функціональними обов’язками та необхідними матеріальними, фінансовими, трудовими та інформаційними ресурсами. Кожне велике підприємство повинно мати у штаті спеціального менеджера з ризику, який розділяє відповідальність за ризиковані рішення з іншими менеджерами

підприємства. Зокрема, ризик-менеджер визначає можливості прийняття або уникнення небажаних ризиків для підприємства.

На цей час існують різні методології, за допомогою яких здійснюється оцінка ризиків. Проведемо аналіз найбільш поширених, а саме:

• аналіз і управління ризиками – методологія, яка використовується у Великобританії – CRAMM;

• оцінка активів та вразливості інформаційної безпеки – OCTAVE;

• управління ризиками в системі інформаційних технологій – NIST SP800-30;

• методи управління ризиками інформаційної безпеки – ISO / IEC 27005: 2011;

• оцінка ризиків інформаційної безпеки – ENISA.

CRAMM реалізує комплексний підхід до оцінки ризиків [1], поєднуючи кількісні та якісні методи оцінки. Метод є універсальним і підходить як для великих, так і для малих організацій, як для урядового, так і для комерційного сектора. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються один від одного своїми базами знань. Для комерційних організацій використовується комерційний профіль (Commercial Profile), а для урядових організацій – урядовий профіль (Government profile).

Методологію OCTAVE створено Software Engineering Institute і Carnegie Mellon University [2]. Вона дозволяє розробити практичні методи й рекомендації для оцінки ризиків. Метод оперативної оцінки критичних ресурсів, загроз, активів і вразливостей (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – це підхід, що визначає стратегію оцінки й планування дій щодо забезпечення безпеки інформації на основі оцінки ризиків.

Методологія оцінки ризиків Національного Інституту Стандартів і Технологій США (National Institute of Standards and Technology – NIST) передбачає виконання таких етапів [3]:

– характеристика системи (активу);

- ідентифікація загроз;
- ідентифікація вразливостей;
- аналіз заходів захисту;
- визначення ймовірності реалізації загроз;
- аналіз збитків (втрат);
- визначення ризиків;
- рекомендації щодо заходів безпеки;
- формування звітної документації.

Вона детально описує всі можливі ризики для інформаційних активів і може використовуватися для підприємств різної величини. Недоліком цієї методології є довготривалий процес аналізу і відсутність автоматизації деяких функцій.

Оцінка ризику IT-підприємства

Оцінка ризику є основним етапом ризик-менеджменту. Організації використовують її для визначення ступеня потенційної загрози. Результат цього процесу допомагає визначити відповідні заходи контролю для зниження або усунення ризиків.

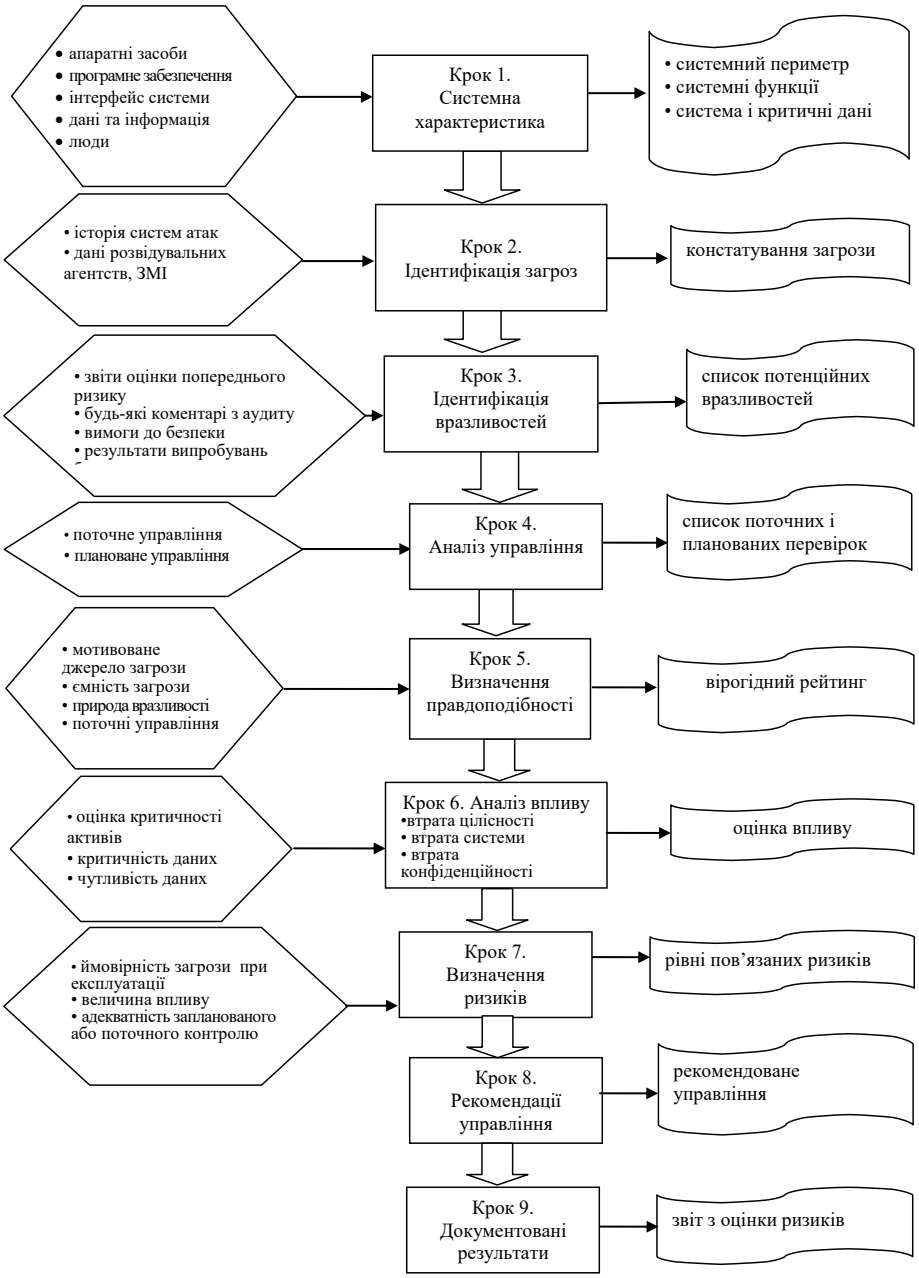


Рисунок 1.3 - Методологія оцінки ризиків інформаційної безпеки

Основні джерела загроз можуть бути природними, антропогенними або екологічними [3].

Навмисний напад може бути шкідливим і полягає в намаганні отримати несанкціонований доступ до IT-системи (наприклад, зламування системи паролів) з метою компрометування системи, порушення цілісності, доступності або конфіденційності даних; а також нешкідливим – для обходження системи безпеки.

Стуктурну схему, в якій наведено методологію оцінки ризиків IT-підприємства подано на рисунку 1.3.

Поняття менеджменту інформаційної безпеки нерозривно пов'язане з ***ризиками*** для інформаційних ресурсів (рисунок 1.4), під якими (ризиками) розуміється можливість (ймовірність) нанесення шкоди інформаційних ресурсів, зниження рівня їх захищеності.

Рисунок 1.4 - Загальна структура менеджменту інформаційної безпеки

Ризики можуть мати різну природу і характеристики; однією з основних класифікацій ризиків для інформаційної безпеки (так само, як і багатьох інших ризиків в економіці та управлінні) є їх поділ:

• на системні ризики - некеровані ризики, пов'язані з тим середовищем і технічною інфраструктурою, в якій функціонують інформаційні системи;

• операційні ризики - як правило, керовані ризики, пов'язані з особливостями використання певних інформаційних систем, їх технічної реалізації, застосовуваними алгоритмами, апаратними засобами і т.п**.**

Основні ризики у сфері МІБ можуть бути розділені на три основних види:

1. порушення конфіденційності інформації;

2. руйнування (втрата, необоротне зміна) інформації;

3. недоступність інформаційних ресурсів - виникнення ситуацій, коли користувачі (всі або їх частину) на деякий період часу втрачають можливість доступу до необхідних даних (або інформаційним системам).

При дослідженні ризику виділяють вразливість і загрози. Спільно ці складові утворюють основу ризику. Загрози без уразливості не є ризиком так само, як і уразливості без погроз. В реальному світі жодна з цих умов не існує. Отже, оцінка ризику - це визначення ймовірності того, що непередбачена подія відбудеться. Ризик якісно визначається трьома рівнями.

Низький. Існує маленька ймовірність прояви загрози. По можливості потрібно почати дії по усуненню уразливого місця, але їх вартість повинна бути зіставлена з малим збитком від ризику.

Середній. Уразливість є значним рівнем ризику для конфіденційності, цілісності, доступності та/або ідентифікації інформації, систем або приміщень організації. Існує реальна можливість здійснення такої події. Дії з усунення вразливості доцільні.

Високий. Уразливість являє собою реальну загрозу для конфіденційності, цілісності, доступності та/або ідентифікації інформації, систем або приміщень організації. Дії з усунення цієї уразливості повинні бути зроблені негайно.

Отже, ризик - це поєднання загрози та вразливості:

$$\textbf{Загроза} + \textbf{Вразливість} = \textbf{Ризик}, \tag{1.1}$$

Вразливість - це потенційний шлях для виконання атаки. Уразливість існує в комп'ютерних системах та мережах (роблячи систему відкритою для атак з використанням технічних методів) або в адміністративних процедурах (роблячи середу відкритою для атак без використання технічних методів чи атак соціального інжинірингу).

Уразливість пов'язана не тільки з комп'ютерними системами та мережами. Безпека будівель і приміщень, питання персоналу і безпека інформації при передачі також вимагають опрацювання.

Безпосереднім джерелом ризиків і негативних впливів є загрози, під якими розуміються потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що порушують інформаційну безпеку. Загроза - це дія або подія, здатне порушити безпеку інформаційних систем. Розглянемо три складових загрози.

1. Цілі. Компонент безпеки, який піддається атаці.

2. Агенти. Люди або організації, що представляють загрозу.

3. Події. Дії, що становлять загрозу.

Розглянемо докладніше кожну із складових.

Цілі. Цілями погроз або нападів в більшості випадків є служби безпеки (див. у "Служби інформаційної безпеки"): служби конфіденційності, цілісності, доступності та ідентифікації. І для цього є реальні підстави.

Конфіденційність стає метою, якщо мотивом є добування інформації несанкціонованими особами або організаціями. У цьому випадку порушник прагне отримати, наприклад, секретні урядові дані. Конфіденційна інформація комерційної організації (відомості про заробітну плату або медичні дані) також може стати метою.

Цілісність є метою, якщо порушник прагне модифікувати інформацію. У цьому випадку він підробляє особисті або інші відомості, наприклад, збільшуючи суму свого банківського рахунку. В іншому випадку метою стає зменшення балансу в журналі банківських операцій або зміна записів у важливій базі даних, щоб викликати сумніви у правильності всієї інформації. Такий підхід стосується компаній, що займаються дослідженням архітектури цифрових мереж.

Доступність стає метою при виконанні атаки на відмову в обслуговуванні. Такі атаки спрямовані на інформацію, додатки, системи або інфраструктуру. Загрози в цьому випадку носять як короткочасний, так і довготривалий характер.

Ідентифікованість сама по собі рідко є метою. Атака на ідентифікованість може бути спрямована на запобігання відновлення організації після інцидентів. Вона вибирається в якості початкового етапу атаки по відношенню до іншим

цілям, таким як приховування змін в базі даних або злом механізмів безпеки, що існують в організації.

Цілей може бути декілька. Наприклад, ідентифікованість служить вихідною метою для запобігання запису дій зловмисника, який порушив конфіденційність секретних даних організації.

Агенти. Агентами загроз є люди, які прагнуть завдати шкоди організації. Для цього вони повинні мати наступне.

• Доступ. Здатність для досягнення мети.

• Знання. Рівень і тип наявної інформації про цілі.

• Мотивація. Причина для знищення цілі.

Доступ. Агент повинен мати доступ до потрібної системі, мережі, обладнання або інформації. Цей доступ буває прямим (наприклад, у нього є обліковий запис у системі) або непрямим (він отримує доступ до обладнання іншим способом). Прямий доступ дозволяє скористатися існуючою вразливістю і, отже, стає загрозою.

Знання. Агент повинен володіти деякими знаннями про цілі:

• ідентифікатор користувача;

• паролі;

• розташування файлів;

• процедури виконання фізичного доступу;

• імена службовців;

• доступні номери телефонів;

• мережеві адреси;

• процедури забезпечення безпеки.

Мотивація. Агенту потрібна мотивація для вчинення дії. Мотивація є спонукає дію, її можна визначити як первинну мету. Мотивацією зазвичай є:

• залучення уваги - бажання похвалитися своїми "перемогами";

• жадібність - жага вигоди (грошей, товарів, послуг або інформації);

• злі наміри, бажання заподіяти шкоду організації або окремій особі.

Події. Події - це способи, за допомогою яких агенти загроз можуть завдати шкоди організації. Наприклад, хакери завдадуть шкоди шляхом зловмисного зміни інформації веб-сайту організації. Слід також взяти до уваги шкоду, що може бути нанесений при отриманні агентом доступу. Необхідно враховувати наступні події:

• зловживання санкціонованим доступом до інформації, систем або сайтів;

• зловмисне зміна інформації;

• випадкове зміна інформації;

• несанкціонований доступ до інформації, систем або сайтів;

• зловмисне руйнування інформації, систем або сайтів;

• випадкове руйнування інформації, систем або сайтів;

• зловмисне фізичне втручання в системи або операції;

• випадкове фізичне втручання в системи або операції;

• природні фізичні події, які заважають систем або операцій;

• введення в дію зловмисного програмного забезпечення (навмисно чи ні);

• порушення внутрішніх або зовнішніх комунікацій;

• несанкціонований пасивний перехват інформації внутрішніх або зовнішніх комунікацій;

• крадіжка апаратного або програмного забезпечення.

Виділяється безліч типів загроз і безліч критеріїв для класифікації загроз інформаційній безпеці. Одним з основних таких критеріїв є розташування джерела порушень до інформаційних ресурсів, щодо яких здійснюється негативний вплив. Відповідно до цього критерію порушення можуть бути розділені:

- на обумовлені внутрішніми факторами (персоналом підприємства, роботою власних інформаційних систем);
- обумовлені зовнішніми факторами (зловмисниками, що не мають безпосереднього відношення до компанії - власника інформаційних активів, природними факторами тощо).

Іншим важливим критерієм є наявність намірів здійснити порушення. Відповідно до нього виділяють:

- цілеспрямовані впливи (можуть бути здійснені як власним персоналом, так і зовнішніми противниками);
- випадкові впливу (помилки користувачів та адміністраторів, збої і випадкові порушення в роботі обладнання, непередбачені впливу природних факторів).

Також можна виділити наступні класифікації загроз:

- по об'єктах (персонал, матеріальні та фінансові кошти, інформація);
- по величині збитку (граничний, значний, незначний);
- по ймовірності виникнення (вельми ймовірні, ймовірні, малоймовірні);
- за типом збитку (моральний, матеріальний) і деякі інші.

Одна з можливих моделей класифікації загроз представлена на рисунку 1.5.

Рисунок 1.5 - Модель можливих загроз системі інформаційної безпеки та основні класи методів захисту

Зазвичай користувачі можуть бути джерелами таких загроз:

1. навмисна (вбудовування логічної бомби, яка з часом зруйнує програмне ядро або програми) або ненавмисна втрата або спотворення даних та інформації,

"злом" системи адміністрування, крадіжка даних і паролів, передача їх стороннім особам і т. д.;

2. небажання користувача працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості або при розходженні між запитами користувачів і фактичними можливостями та технічними характеристиками) і навмисне виведення з ладу її програмно-апаратних пристроїв;

3. неможливість працювати з системою в силу відсутності відповідної підготовки (недолік загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією тощо).

Очевидно, що ефективний спосіб боротьби з ненавмисними помилками — максимальна автоматизація і стандартизація, інформаційних процесів, використання пристроїв "захист від дурня" (Fool Proof Device), регламентація і строгий контроль дій користувачів. Необхідно також стежити за тим, щоб при звільненні працівника його права доступу (логічного і фізичного) до інформаційних ресурсів анулювалися.

Результати проведення оцінки ризику та аналізу загроз можуть бути використані при виборі адекватних оптимальних методів парирування загроз, а також при аудиті реального стану інформаційної безпеки об'єкта. Один з можливих алгоритмів проведення такого аналізу, який легко формалізується і алгоритмизируется. Завдяки такому підходу можливо:

• встановити пріоритети цілей безпеки для суб'єкта відносин;

• визначити перелік актуальних джерел загроз;

• визначити перелік актуальних вразливостей;

• оцінити взаємозв'язок вразливостей, джерел загроз і можливості їх здійснення;

• визначити перелік можливих атак на об'єкт;

• розробити сценарії можливих атак;

• описати можливі наслідки реалізації загроз;

• розробити комплекс захисних заходів і систему управління інформаційною безпекою підприємства.

1.3 Порівняльний аналіз існуючих систем захисту конфіденційної інформації в приватних організаціях

Переваги використання СВА порівняно з firewall’ами

Кожен засіб захисту адресовано конкретній загрозі в системі. Більше того, кожен засіб захисту має слабкі та сильні сторони. Тільки комбінуючи їх, можна захиститися від максимально великого спектру атак.

Firewall’и є механізмами створення бар’єру, заступаючи вхід деяких типів мережевого трафіку і дозволяючи інші види трафіку. Створення такого бар’єру відбувається на основі політики firewall’а. Системи виявлення атак служать механізмами моніторингу, спостереження активності та прийняття рішень про те, чи є спостережувані події підозрілими. Вони можуть виявити атакуючих, які обійшли firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить кроки щодо запобігання атаки.

Системи виявлення атак стають необхідним доповненням інфраструктури безпеки в кожній організації. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від систем виявлення атак існує, і не маленька, що доведено експертним методом оцінювання у таблиці 1.2.

Таблиця 1.1 - Порівняння методів СВА

Характеристика	Сигнатурні методи	Методи аномалій
Множина атак	виявлення обмежується відомими видами	Обмеження можливостями налаштування і методами аналізу
Ймовірність пропуску атаки	Середня	СВА низька
Ймовірність помилкового спрацювання	Дуже низька	Висока
Вимоги до обчислювальних ресурсів	Середні	Високі

Важливим елементом в системах виявлення атак є швидкість реакції,що відбувається через певні проміжки часу, тобто пакетно. Швидкість реакції вказує на час, що минув між подіями, які були виявлені монітором, аналізом цих подій і реакцією на них.

У системах, реакція яких відбувається через певні проміжки часу, інформаційний потік від точок моніторингу до інструментів аналізу не є безперервним. У результаті інформація обробляється способом, аналогічним комунікаційним схемами "зберегти і перенаправляти". Багато ранніх host-based систем виявлення атак вико- ристовують дану схему хронометражу, тому що вони залежать від записів аудиту в ОС. Засновані на інтервалі системи не виконують ніяких дій, які є результатом аналізу подій.

Real-Time (безперервні) системи виявлення атак обробляють безперервний потік інформації від джерел. Найчастіше це є домінуючою схемою в network-based системах, які отримують інформацію з потоку мережевого трафіку. Термін "реальний час"використовується в тому ж сенсі, що і в системах управління процесом. Це означає, що визначення проникнення, що виконується системами виявлення атак в "реальному часі призводить до результатів досить швидко, що дозволяє виконувати певні дії в автоматичному режимі.

Таблиця 1.2 - Імовірності подолання загроз різними засобами захисту

	Міжмереже-вий екран	VPN шлюз	СВА	Антивірус
Троянські програми				0,96
Віруси				0,92
DoS-атаки	0,81	0,98	0,98	
DDoS-атаки	0,62	0,79	0,97	
Макровіруси				0,6
IP Spoofing	0,69	0,96	0,95	
DNS Spoofing			0,92	
WEB Spoofing			0,54	
Захоплення мережевих підключень	0,51	0,97	0,93	
Різні сканування мережі	0,59		0,89	
Порушення конфіденційності даних		0,95		
Автоматичний підбір паролів	0,75		0,91	
Атаки на протоколи			0,79	
Неавторизоване використання прав	0,32		0,91	
Неконтрольоване використання ресурсів	0,53	0,61	0,81	0,64
Неавторизоване використання АС	0,62	0,73	0,79	0,67
Прослуховування мережі		0,92		
Шпигунське ПЗ			0,54	0,97

Вибір СВА повинен ґрунтуватись на вимогах, що висуваються до системи захисту інформації в кожному конкретному випадку. Проведене дослідження та порівняльний аналіз сучасних систем виявлення атак та запобігання вторгненням

показав, що при вдосконаленні існуючих та проектуванні нових систем необхідно враховувати визначені властивості, зважаючи на особливості реалізації та функціонування інформаційної системи, які підлягають захисту.

Висновки до розділу 1

На цей час актуальним є питання забезпечення інформаційної безпеки. В свою чергу, для забезпечення інформаційної безпеки як окремих підприємств, так і держави в цілому важливим є питання оцінки ризиків, які виникають в процесі діяльності підприємств. Для оцінки ризиків інформаційної безпеки використовуються різні методики і стандарти управління інформаційними ризиками (УІР).

На цей час існують різні методології, за допомогою яких здійснюється оцінка ризиків. Було проведено аналіз найбільш поширених, а саме:

• аналіз і управління ризиками – методологія, яка використовується у Великобританії – CRAMM;

• оцінка активів та вразливості інформаційної безпеки – OCTAVE;

• управління ризиками в системі інформаційних технологій – NIST SP800-30;

• методи управління ризиками інформаційної безпеки – ISO / IEC 27005: 2011;

• оцінка ризиків інформаційної безпеки – ENISA.

Кожен засіб захисту адресовано конкретній загрозі в системі. Більше того, кожен засіб захисту має слабкі та сильні сторони. Тільки комбінуючи їх, можна захиститися від максимально великого спектру атак.

2 ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ПРИВАТНИХ ОРГАНІЗАЦІЯХ

2.1 Постановка задачі та вибір інструментів її реалізації

Розвиток підходів до рішення проблеми захисту інформації проходив від забезпечення захисту лише формальними механізмами, що містять головним чином технічні й програмні засоби в рамках ОС і СУБД, через виділення керуючого компонента, ядра безпеки, і розвиток неформальних засобів захисту до формування погляду на захист як на неперервний процес, до розвитку стандартів, посиленню тенденції апаратної реалізації функцій захисту, формуванню висновку про взаємозв'язок захисту інформації, архітектури систем обробки даних і технології їх функціонування, до формування *системного комплексного підходу*, що є визначальним на сучасному етапі розвитку [3,4,23].

Систематизація відомостей про забезпечення безпеки інформаційних технологій, питання взаємодії при функціонуванні конкретних механізмів захисту інформації необхідно приводять до висновку про обов'язковість вимоги системності підходу до захисту інформації як регулярного процесу, здійснюваного на всіх етапах життєвого циклу інформаційної системи, зневага яким безпосередніми користувачами завдає значної шкоди інформації, яка захищається [1,2].

Під *системністю* розуміється пояснювальний принцип наукового пізнання, що вимагає дослідження явищ у їхній залежності від внутрішньо зв'язаного цілого, яке вони утворюють, здобуваючи завдяки цьому притаманні цілому нові властивості. Використання цього основного принципу в теорії захисту інформації дає можливість для наукового обґрунтування структуризації процесів захисту, враховуючи їх взаємозв'язок і взаємовплив.

Під комплексністю системи захисту інформації розуміється комбінація наступних заходів [3,4]:

- Законодавчі заходи. Використання законодавчих актів, що регламентують права й обов'язки фізичних і юридичних осіб, а також держави в області захисту інформації;
- Морально-етичні заходи. Створення й підтримка на об'єкті такої моральної атмосфери, у якій порушення регламентованих правил поведінки оцінювалося б більшістю співробітників негативно;
- Фізичні заходи. Створення фізичних перешкод для доступу сторонніх осіб до охоронюваної інформації;
- Адміністративні заходи. Організація відповідного режиму таємності, пропускного й внутрішнього режиму;
- Технічні заходи. Застосування електронних і інших засобів для захисту інформації;
- Криптографічні заходи. Застосування шифрування й кодування для приховування оброблюваної й переданої інформації від несанкціонованого доступу;
- Програмні заходи. Застосування програмних засобів розмежування доступу.

Перераховані заходи у своїй комбінації необхідно приводять до висновку, що комплексність системи захисту інформації може бути досягнута лише при взаємоузгоджуваній участі в рішенні відповідних задач професіоналів — керівників, фахівців, які задіяні в процесах збору, передачі, зберігання, обробки й використання інформації, а ефективне вирішення проблем захисту можливо тільки при наявності розвиненого й адекватного наукового базису.

Системно-концептуальний підхід [4], визначає основні вимоги до комплексних систем захисту інформації, серед яких:

- використання комплексу програмно-технічних засобів і організаційних заходів;
- надійність, продуктивність, конфігурованість;
- економічна доцільність;
- можливість удосконалювання;

- забезпечення розмежування доступу до конфіденційної інформації з відволіканням порушника на хибну інформацію;
- взаємодія з незахищеними комп'ютерними мережами за встановленими для цього правилами розмежування доступу;
- забезпечення проведення обліку й розслідування випадків порушення безпеки інформації в комп'ютерних мережах і т.д.

Огляд сучасного стану й шляхів розвитку методів і засобів інформаційної безпеки [3,4], проведений з використанням єдиного системно-концептуального підходу, приводить до виділення в предметній галузі захисту інформації (ЗІ) трьох ієрархій: структурної (рисунок 2.1), причинно-наслідкової (рисунок 2.2) і функціональної (рисунок 2.3), що структурує і значно полегшує вивчення й аналіз процесів у даній галузі.

Подальше вдосконалювання теорії захисту очевидно пов'язане з обліком нових обставин, характерних для сучасного періоду розвитку інформатизації суспільства:

Спостережувані в останні роки тенденції в розвитку інформаційних технологій ведуть до появи якісно нових (інформаційних) форм боротьби, у тому числі й на міждержавному рівні. У силу цього все більшу актуальність здобуває не тільки захист інформації, але й захист людей і технічних (головним чином, електронних) систем від руйнуючого впливу інформації, у зв'язку із чим формується задача забезпечення інформаційної безпеки як органічної сукупності задач захисту інформації й захисту від інформації . Захист від інформації полягає у використанні спеціальних методів і засобів з метою попередження або нейтралізації негативного впливу на елементи системи (людей і технічні комплекси) інформації, як наявної всередині системи (генеруємої, збереженої, оброблюваної й використовуваної), так і тої, що надходить з зовнішнього середовища (захист системи від інформації), а також попередження негативного впливу вихідної інформації системи на елементи зовнішнього середовища (інформаційна екологія). Актуальність цієї частини загальної проблеми інформаційної безпеки полягає в тому, що інформація здатна так впливати на

людей і технічні комплекси, що результати можуть носити не просто негативний, а трагічний і навіть катастрофічний характер;

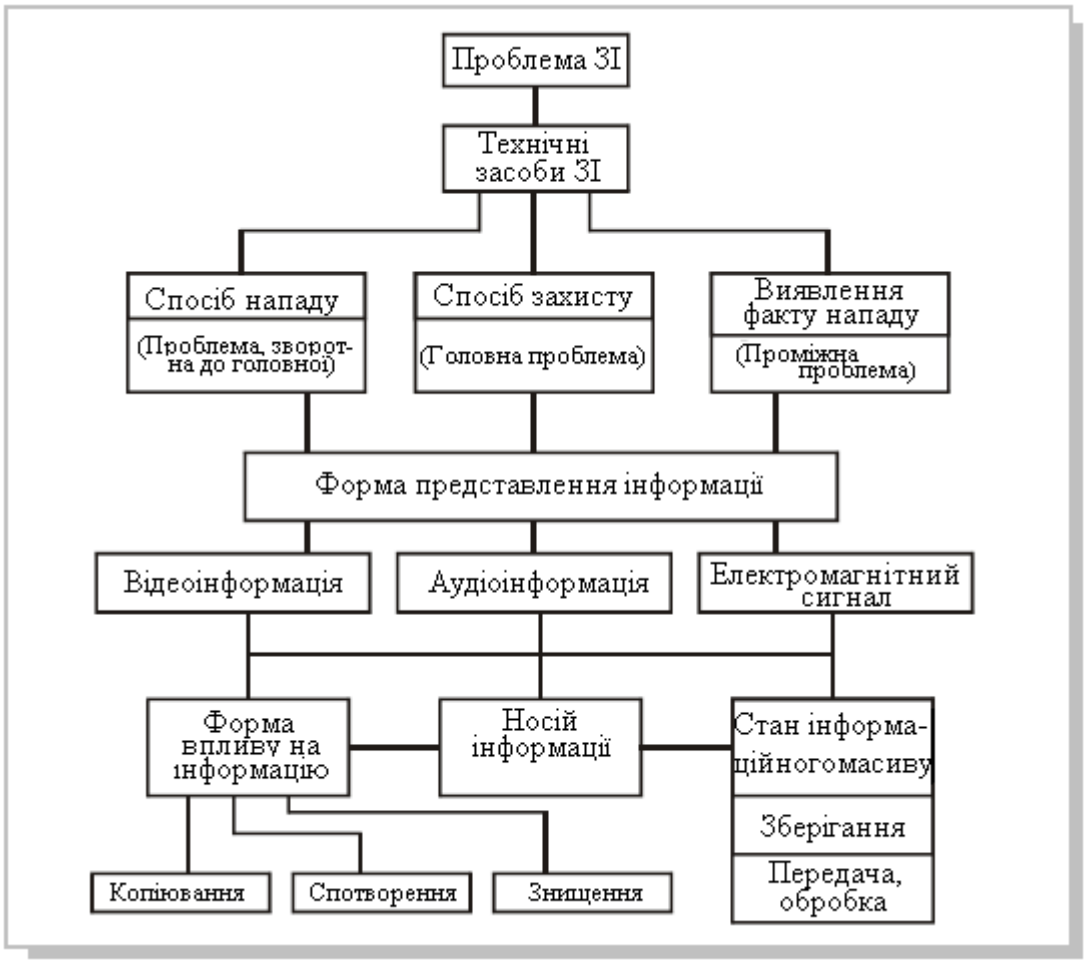


Рисунок 2.1 - Семантична схема проблеми захисту інформації з позицій структурної ієрархії

- З самого початку регулярного використання автоматизованих технологій обробки інформації актуальною є задача забезпечення необхідної якості інформації. Із часом актуальність даної задачі зростає, а сама задача ускладнюється;
- Основна увага на новому етапі розвитку теорії захисту інформації повинна приділятися вдосконалюванню науково-методологічного базису й інструментальних засобів, що забезпечують рішення будь-яких виникаючих задач на регулярній основі.

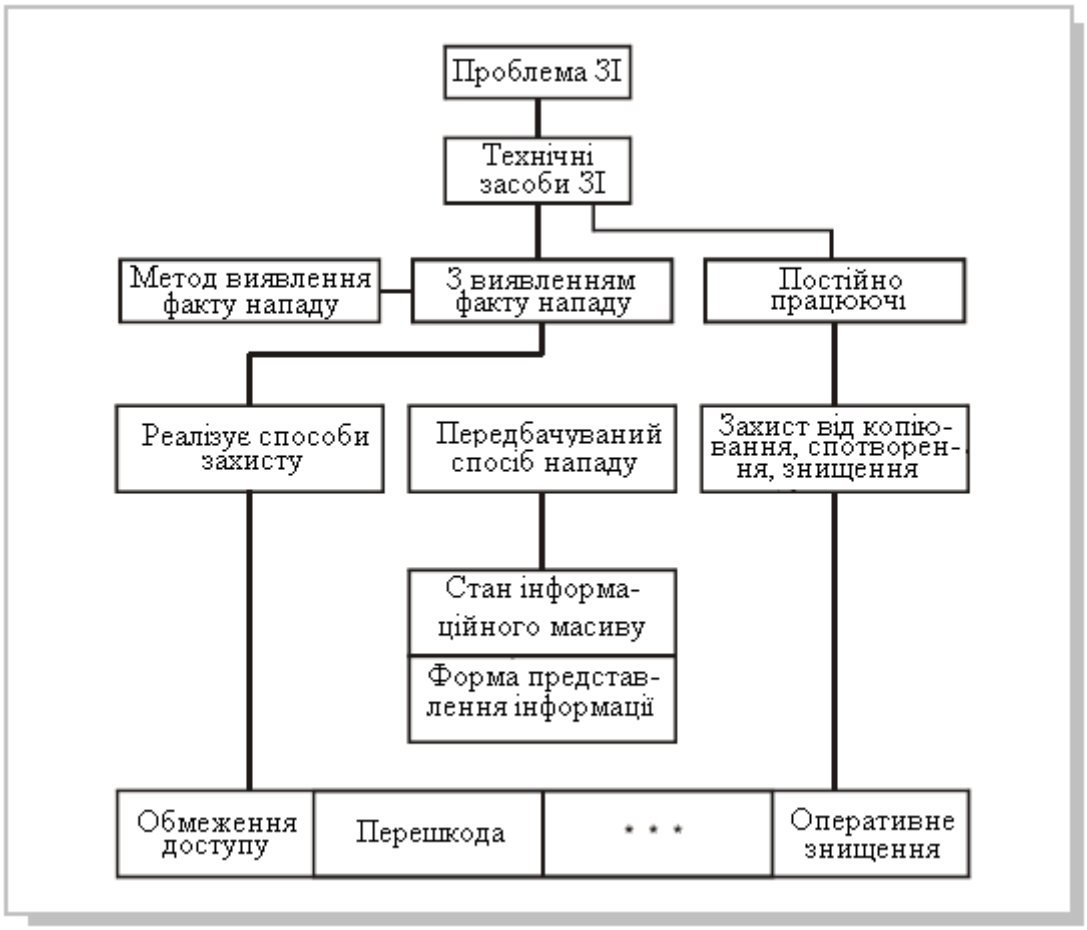


Рисунок 2.2 - Семантична схема проблеми захисту інформації з позицій причинно-наслідкової ієрархії

Поглиблене вивчання проблеми вдосконалювання науково-методологічного базису теорії захисту інформації привело до висновку, що вже в цей час і в перспективі вирішення проблем захисту поза органічним зв'язком з рішенням більш загальних проблем (інформаційних технологій, інформатизації суспільства і т.д.) може привести до неадекватних результатів. Серйозність даного питання визнана настільки ґрунтовною, що його рішення повинне вестися з використанням інших, у порівнянні з колишніми, інтенсивних підходів. Інтенсивний підхід припускає організацію захисту інформації на всіх об'єктах відповідно до деякої єдиної, науково обґрунтованої концепції, на відміну від екстенсивного підходу, який у своєму «чистому виді» означає незалежну

організацію захисту на кожному об'єкті. Перехід до інтенсивних способів захисту означає цілеспрямовану реалізацію всіх досягнень теорії й практики в області інформаційної безпеки. Можна виділити наступні основні положення, практична реалізація яких означає перехід до інтенсивних способів захисту інформації:

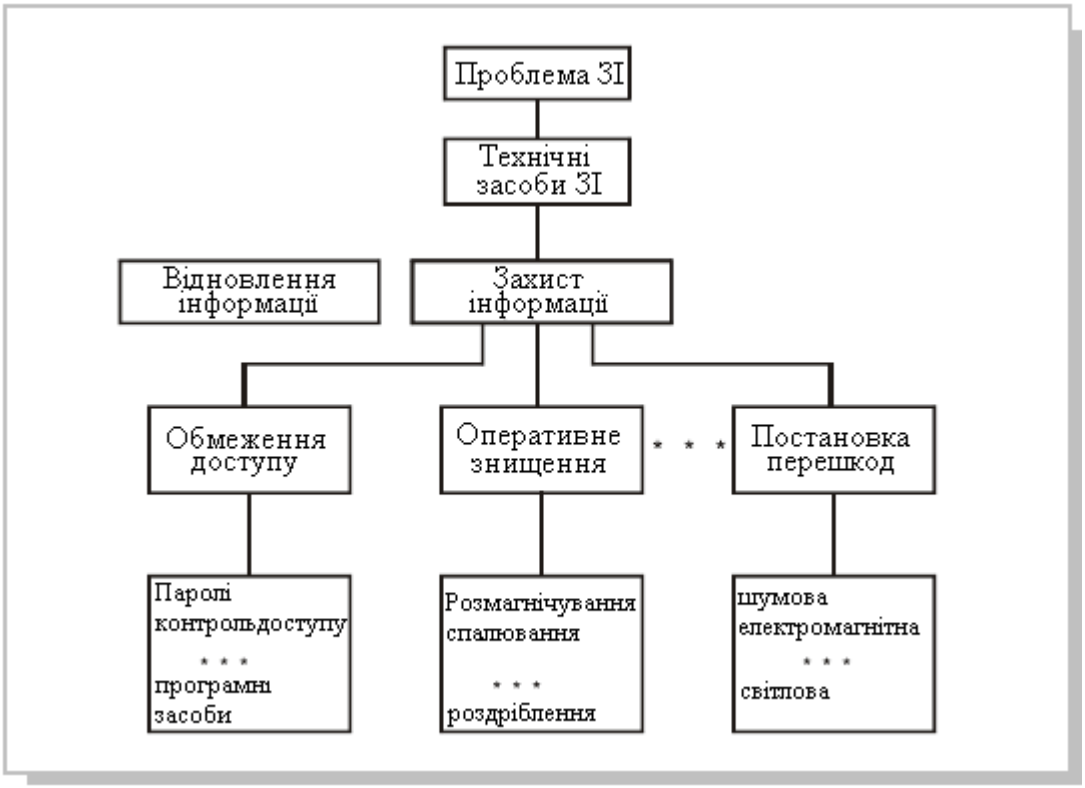


Рисунок 2.3 - Семантична схема проблеми захисту інформації з позицій функціональної ієрархії

- Структурований опис середовища захисту, який неодмінно робиться перед безпосереднім рішенням питань захисту. Такий опис представляє структуру об'єкта, що захищається, і технологію обробки інформації на ньому;
- Всебічний і кількісний аналіз ступеня вразливості інформації на об'єкті. Такий аналіз необхідний для більш об'єктивної оцінки реальних загроз інформації й необхідних зусиль і витрат на її захист. Можливе використання, наприклад, методології оцінки вразливості інформації, що містить три елементи :

- системи показників вразливості,
- системи загроз інформації,
- системи моделей визначення поточних і прогнозування очікуваних значень показників вразливості.

Однак необхідно відзначити, що практична реалізація запропонованої методології потребує подолання великих труднощів, пов'язаних з формуванням баз вхідних даних, необхідних для забезпечення моделей оцінки вразливості;

- Науково обґрунтоване кількісне визначення необхідного рівня захисту на кожному конкретному об'єкті й у конкретних мінливих умовах його функціонування.

Практична реалізація переходу до інтенсивних способів захисту неможлива без всебічної розробки теоретичних основ побудови систем захисту інформації, які є дуже складними й, незважаючи на активні дослідження в цій предметній галузі, ще далекі від досконалості, без залучення численних і різноманітних математичних інструментів для формального представлення інформаційних систем і організації ефективного аналізу їх стану й технології функціонування.

Одна зі спроб формалізації аналізу систем захисту інформації в електронних системах обробки даних була зроблена А.А.Грушо , де як основний математичний інструмент використовується дискретна математика. Основним методом для рішення задач аналізу й синтезу інформаційних систем виступає ієрархічний метод, що дозволяє максимально наблизити проведені теоретичні дослідження до їхньої практичної реалізації в процесі створення автоматизованих інформаційних систем, що вимагають проектування, побудови, підтримки в працездатному стані великого програмно-апаратного комплексу. Складність цих систем така, що потрібна розробка спеціальної технології проектування й їх побудови, основним інструментом якої і є ієрархічний метод.

Для проведення досліджень і одержання практичних результатів в об'єкт дослідження за назвою інформація вноситься структура мови (мова — множина правильних слів у деякому алфавіті), що має штучний характер, але дозволяє

говорити про інформацію як про дискретну систему. Основою для формалізації є представлення інформації й стану будь-якого обладнання в обчислювальній системі у вигляді слова. Перетворення інформації й зміна стану обладнання представляє відображення слова в інше слово використовуваної мови, що дає можливість узагальнити поняття інформаційного перетворення. Однак у запропонованого підходу є ряд суттєвих недоліків:

- Спосіб моделювання перетворення інформації й системи не дає можливості визначити силу перетворюючої дії на розглянуті об'єкти, ступінь зміни об'єктів, тобто наслідку дій;
- Опис перетворення даних є словом мови. Це не дає можливості динамічної зміни множини можливих перетворень, тому що нове перетворення може не виявитися правильним словом у алфавіті;
- По наявних описах об'єктів у вигляді слів неможливо однозначно визначити, чи різним об'єктам відповідають ці описи або різним станам одного об'єкта;
- При описі стану об'єкта у вигляді слова не можна зробити висновок про те, наскільки стан об'єкта стійкий, чутливим або нечутливим є об'єкт до збурних дій;
- Скрутним є введення поняття відстані (метрики) між різними об'єктами (різними станами об'єктів), що дозволив би адекватно оцінювати ступінь близькості між ними.

Наведені недоліки роблять запропонований підхід неспроможним для рішення питань всебічного аналізу стану систем захисту інформації з використанням їх формального представлення.

Формалізація аналізу інформаційних систем необхідна також для побудови оптимальної, тобто такої, яка в передбачуваних умовах щонайкраще задовольняє умовам розглянутої задачі, системи захисту інформації. Добре відомі труднощі при створенні такої системи:

- наявність цілеспрямованої протидії з боку протиборчої системи, способи дій якої невідомі дослідникові;
- недостатня вивченість деяких явищ, що супроводжують процес функціонування системи захисту;

- нечітке уявлення мети операції;
- складний опосередкований взаємозв'язок показників якості системи захисту інформації з показниками якості інформаційної системи;
- необхідність врахування великої кількості показників (вимог) системи захисту інформації при оцінці й виборі їх раціонального варіанта;
- переважно якісний характер показників (вимог), що враховуються при аналізі й синтезі системи захисту інформації, взаємозв'язок і взаємозалежність цих показників (вимог), які мають суперечливий характер;
- труднощі при одержанні вхідних даних, необхідних для рішення задач аналізу й синтезу систем захисту інформації, особливо на ранніх етапах їх проектування.

Хоча все це робить неефективним застосування традиційних в області інформаційної безпеки математичних інструментів, таких як методи математичної статистики й теорії ймовірностей, а також класичних методів оптимізації для рішення задач моделювання, аналізу й синтезу систем захисту інформації, такі спроби все-таки робляться.

Так пропонується узагальнена модель процесів захисту інформації. Оптимальність системи інтерпретується відповідно до загальних постановок оптимізаційних задач: при заданих ресурсах забезпечити досягнення максимального результату або забезпечити досягнення заданого результату при мінімальній витраті ресурсів. Таким чином, у кожному разі тут йдеться лише про найбільш раціональне використання ресурсів, виділюваних або необхідних для захисту інформації. Наведена модель ніяк не відображає апріорну стійкість наявної системи до можливих загроз, ступінь її «руйнувань» при застосуванні тих або інших загроз. Крім того, щоб реально скористатися цією узагальненою моделлю повинні бути відомі функціональні залежності значень введених в показників захищеності від параметрів системи й зовнішнього середовища й залежність самих параметрів від розмірів ресурсів, вкладених у відображувані ними процеси. Однак строге виконання цих вимог практично неможливе, експертні ж оцінки не гарантують необхідної точності, що є серйозним недоліком запропонованої узагальненої моделі процесів захисту інформації.

Широко розповсюдженим і часто використовуваним у сучасних наукових роботах, присвячених рішенню задач аналізу, синтезу й моделювання інформаційних систем і систем захисту інформації, є підхід, що базується на теорії нечітких множин. На перший погляд, це обґрунтовано й логічно. На відміну від математичної статистики й теорії ймовірностей, що використовують експериментальні дані, володіють певною точністю й вірогідністю, теорія нечітких множин має справу з «людськими знаннями», які називаються експертною інформацією. Основні положення теорії нечітких множин, що мають принципове значення для рішення задач захисту інформації в сучасній їхній постановці.

Апарат нечітких множин і нечіткої логіки застосовується для рішення задач, у яких вхідні дані погано формалізовані. До таких задач належать й задачі області інформаційної безпеки. Сильними сторонами такого підходу є:

- опис умов і методу рішення задачі мовою, близькою до природної;
- універсальність: згідно зі знаменитою теоремою, доведеною Б.Коско в 1993 р., будь-яка математична система може бути апроксимована системою, заснованою на нечіткій логіці;
- ефективність (пов'язана з універсальністю), що пояснюється сукупністю теорем, аналогічних теоремам про повноту для штучних нейронних мереж.

Однак, математична модель, побудована на базі нечітких множин, не може бути позбавлена недоліків самої теорії. Теорії нечітких множин притаманні такі особливості, які приводять до принципових проблем у процесі використання її як інструмента моделювання невизначених параметрів складних систем. На ці проблеми не один раз звертали увагу як прихильники, так і супротивники цієї теорії . Аксіоматичні основи теорії нечітких множин не дозволяють знайти таку інтерпретацію ступеня приналежності нечіткій множині, щоб одержати об'єктивне джерело (або розрахунковий алгоритм) для визначення відповідних функцій приналежності, як це має місце, наприклад, для функцій розподілу ймовірностей у теорії ймовірностей. Тому експертні оцінки становлять єдине джерело одержання функцій приналежності нечітких множин, а сама функція

приналежності представляє суб'єктивну міру відповідності елемента множині. Крім того, аксіоматика теорії реалізована так, що ця теорія не має істотних формальних засобів для обмеження впливу суб'єктивних рішень експерта на результат визначення функції приналежності й формального контролю несуперечності цих рішень, як це має місце в тій же теорії ймовірностей. У випадку теорії нечітких множин значення функції приналежності й співвідношення між ними формально можуть бути довільними. Тому отримані в такий спосіб результати залежать як від самого експерта, так і від методу проведення експертної процедури.

Для часткового усунення зазначених недоліків деякими авторами було запропоновано робити нечіткі керуючі системи адаптивними, коректуючи в процесі роботи правила, параметри функцій приналежності й самі системи, що надзвичайно ускладнює процес практичної реалізації такої системи й може привести завдяки цьому до недоцільності використання корекції. Одним з варіантів запропонованої адаптації є метод гібридних нейронних мереж. Гібридна нейронна мережа ідентична по своїй структурі багатошаровій нейронній мережі з навчанням, наприклад, за алгоритмом зворотного поширення помилки, але сховані шари в ній відповідають етапам функціонування нечіткої системи.

Ідея адаптивності разом з її негативними сторонами перекликається з ідеєю про те, що оцінки параметрів системи захисту інформації в умовах високого ступеня невизначеності її функціонування повинні отримуватися з використанням не однієї математичної моделі, а погодженої сукупності моделей, що адаптивно конструюються одна з іншої і безупинно удосконалюються на основі оптимального вибору вхідних даних [1,2], забезпечення й реалізація якого викликає значні труднощі.

Для створення адекватної моделі надзвичайно важливо враховувати, що будь-яка інформаційна система є системою в загальному виді, тобто формально інформаційна система *S* — це об'єкт, що існує в часі, що зазнає внутрішніх і зовнішніх дій (*збурень*), реагуючий на них змінами своїх станів, й здатний

проявити в тому або іншому виді ці реакції. Тому будь-яка інформаційна система має наступні ознаки :

- Має штучну, антропогенну природу — створюється людьми;
- Має цілісність — усі її частини працюють для досягнення єдиної мети функціонування. Формулювання мети функціонування, визначення кількісних показників досягнення цієї мети (цільова функція) і вимірних характеристик якості функціонування (критеріїв ефективності) не можуть бути задані зсередини системи. Усі ці показники й характеристики визначаються зовнішнім стосовно системи середовищем;
- Сукупність елементів, що складають інформаційну систему, мають різноманітні виконувані функції, різну складність і вартість;
- Система завжди є складною в тому розумінні, що всі її елементи впливають один на одного, і зміна стану одного з них викликає зміни станів інших. При цьому кількісні характеристики взаємного впливу елементів не обов'язково мають властивість лінійності. Ці залежності можуть бути нелінійними, немонотонними;
- Практично всі інформаційні системи є автоматизованими: частина їх функцій виконується людиною, а частина — технічним обладнанням;
- Інформаційні системи функціонують у конкурентному середовищі, тому їх робота супроводжується конфліктними ситуаціями.

Незважаючи на відповідність ознак інформаційної системи й системи в загальному виді, у зв'язку з тим, що процеси захисту інформації піддаються впливу випадкових факторів, методи класичної теорії систем також виявляються практично непридатними для використання як основи загального підходу до аналізу стану й технології функціонування інформаційних систем. Питання, пов'язані з актуальною необхідністю розширення використовуваного тут донедавна математичного апарату, вже не раз піднімалися у відкритих джерелах. Однак пропоновані «розширення» не виходили за межі евристичного програмування, психоінтелектуальної генерації, методів нечітких множин, лінгвістичних змінних (нестрогої математики), неформального оцінювання, неформального пошуку оптимальних рішень [1,2] і ін., основні недоліки яких

обговорювалися вище, і, на думку авторів даної роботи, принципово не могли привести до створення адекватного математичного базису для комплексного рішення поставлених задач.

З кінця минулого століття в теорії керування почав розвиватися й залишається найбільш перспективним на сьогоднішній день «некласичний» підхід при моделюванні систем захисту інформації, що ґрунтується на аналогіях архітектури й цілей функціонування складних технічних і біологічних систем, що є природними системами керування [12]. Основна ідея тут полягає в наступному: проблему забезпечення безпеки складних автоматизованих і телекомунікаційних систем необхідно вирішувати, орієнтуючись на організацію біологічних систем, що мають високу захищеність. Як біологічним, так і складним технічним системам властивий ієрархічний принцип організації. Крім того, обом видам систем властива спільність цілей: підтримка життєздатності складної системи протягом тривалого часу за рахунок забезпечення надійного кодування, зберігання, перетворення й передачі інформації. Додання технічним системам позитивних якостей біосистем, відповідальних за безпеку й надійність інформаційних процесів, дозволить змінити сам підхід до створення складних комп'ютерних систем, систем захисту інформації.

2.2 Розробка методики захисту конфіденційної інформації

Сучасний розвиток технологій Internet / Intranet призводить до необхідності захисту інформації, переданої в рамках розподіленої корпоративної мережі, яка використовує мережі відкритого доступу. Виділені канали може собі дозволити далеко не будь-яка компанія, тому найчастіше використовується Internet.

В абсолютній більшості випадків відповідь захищатися треба - від зовнішніх зловмисників: хакерів, від звільнених або скривджених співробітниками компанії і насамперед від тих, хто наділений великими повноваженнями (аналітики, розробники, системні адміністратори), які знають паролі до всіх систем, що використовуються в організації.

Необхідно захищатися від

• від порушення інформаційних канал і ресурсів;

• від несанкціонованого доступу до інформації, що приводить до порушення її цілісності;

• від руйнування засобів захисту що вбудовані, призначених для доказу неправомочність дій користувачів і обслуговуючого персоналу;

• від впровадження "вірусів" і "закладок" в програмні продукти та технічні засоби.

Як захищатися?

У всьому світі зараз прийнято будувати комплексну систему захист інформації та інформаційних систем у кілька етапів - на основі формування концепції інформаційної безпеки.

Перший етап - інформаційне обстеження підприємства - найважливіший. Саме на цьому етапі визначається, від чого в першу чергу необхідно захищатися компанії.

Спочатку будується так звана модель порушника, яка описує ймовірний вигляд зловмисника, тобто його кваліфікацію, наявні засоби для реалізації тих

чи інших атак, звичайний час дії і т. п. За результатами етапу виробляються рекомендації щодо усунення виявлених загроз, правильному вибору і застосування засобів захисту.

Поряд з аналізом існуючої технології повинна здійснюватися розробка політики в області інформаційної безпеки і зводу організаційно-розпорядчих документів, які є основою для створення інфраструктури інформаційної безпеки (ІБ) (рисунок 2.4).

Рисунок 2.4 - Складові інфраструктури інформаційної безпеки

Формування політики ІБ має зводитися до наступних практичних кроків.

1. Визначення та розробка керівних документів і стандартів в області ІБ, а також основних положень політики ІБ, включаючи:

о принципи адміністрування системи ІБ та управління доступом до обчислювальних і телекомунікаційних засобів, програмами, а також доступом до приміщень, де вони розташовуються;

о принципи контролю стану систем захисту інформації, способи інформування про інциденти в області ІБ та вироблення корегуючих заходів, спрямованих на усунення загроз;

о принципи використання інформаційних ресурсів персоналом компанії і зовнішніми користувачами;

о організацію антивірусного захисту і захисту проти несанкціонованого доступу та дій хакерів;

о питання резервного копіювання даних та інформації;

о порядок проведення профілактичних, ремонтних та відновлювальних робіт;

о програму навчання та підвищення кваліфікації персоналу.

2. Розробка методології виявлення та оцінки загроз та ризиків їх здійснення, визначення підходів до управління ризиками: чи є достатнім базовий рівень захищеності або потрібно проводити повний варіант аналізу ризиків.

3. Структуризацію контрзаходів за рівнями вимог до безпеки.

4. Порядок сертифікації на відповідність стандартам у галузі ІБ. Повинна бути визначена періодичність проведення нарад за тематикою ІБ на рівні керівництва, включаючи періодичний перегляд положень політики ІБ, а також порядок навчання всіх категорій користувачів інформаційної системи з питань ІБ.

Наступним етапом побудови комплексної системи інформаційної безпеки служить придбання, встановлення та налаштування рекомендованих на попередньому етапі засобів і механізмів захисту інформації.

До таких засобів можна віднести системи захисту інформації від несанкціонованого доступу, системи криптографічного захисту, міжмережеві екрани, засоби аналізу захищеності та інші.

Чим захищатися?

Умовно можна виділити три категорії засобів захисту - традиційні засоби, нові технології та засоби криптографічного захисту інформації.

Криптографічні засоби

Криптографічні засоби призначені для захисту критично важливих даних від несанкціонованого прочитання і / або модифікації.

Формальні математичні методи криптографії були розроблені Клодом Шенноном [Шеннон К. Математична теорія криптографія, 1945]. Він довів теорему про існування та єдність абсолютно стійкого шифру - такої системи шифрування, коли текст одноразово зашифровується за допомогою випадкового відкритого ключа такої ж довжини.

У 1976 році американські математики У. Діффі та М. Хеллман обгрунтували методологію асиметричного шифрування з застосуванням відкритої односпрямованої функції (це така функція, коли за її значенням можна відновити значення аргументу) та відкритої односпрямованої функції з секретом.

У 1990-і роки в США були розроблені методи шифрування з допомогою особливого класу функцій - хеш-функцій (Hash Function). Хеш-функція (дайджест-функція) - це відображення, на вхід якого подається повідомлення змінної довжини M, а виходом є рядок фіксованої довжини h (M) - дайджест повідомлення. Крипостійкість такого методу шифрування полягає в неможливості підібрати документ M ', який володів би необхідним значенням хеш-функції. В даний час на цих принципах будуються алгоритми формування електронного цифрового підпису (ЕЦП).

Найбільш використовуваними симетричними алгоритмами шифрування в даний час є DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), RC2, RC5, CAST, Blowfish. Асиметричні алгоритми - RSA (Rivest, Shamir, Adleman), алгоритм Ель Гамаля, криптосистема ECC на еліптичних кривих, алгоритм відкритого розподілу ключів Діффі-Хеллмана. Алгоритми, засновані на застосуванні хеш-функцій, - MD4 (Message Digest 4), MD5 (Message Digest 5), SHA (Secure Hash Algorithm).

Найбільш відомим програмним продуктом, поширюваним вільно, є пакет PGP (Pretty Good Privacy). (1995 Філом Циммерманом), який використовував згадані вище алгоритми RSA, IDEA, і MD5.

PGP складається з трьох частин - алгоритму IDEA, сигнатури та цифрового підпису. PGP використовує три ключі - відкритий ключ адресата, секретний

ключ власника і сеансовий ключ, що генерується за допомогою RSA і відкритого ключа випадковим чином при шифруванні повідомлення (рисунок 2.5).

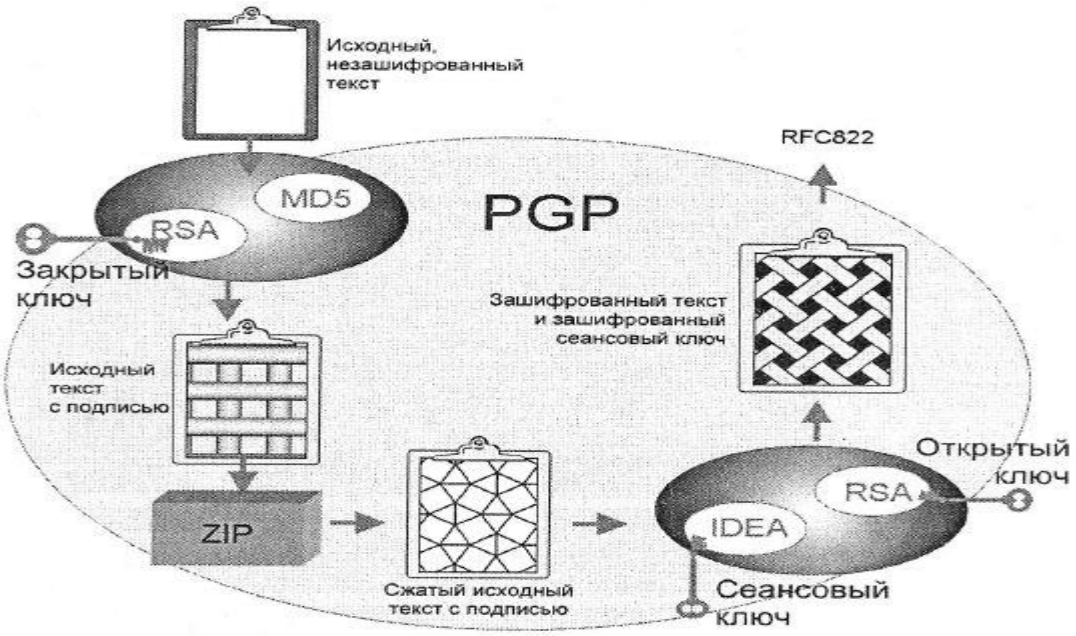


Рисунок 2.5 - Схема формування захищеного повідомлення за допомогою пакету PGP

Системи розмежування доступу і міжмережеві екрани (розмежовують доступ між двома ділянками мережі з різними вимогами щодо безпеки). З міжмережевих екранів можна назвати продукти компаній CheckPoint і CyberGuard - Firewall-1 і CyberGuard Firewall). До класу міжмережевих екранів можна також віднести і багато маршрутизатори, реалізують фільтрацію даних на основі спеціальних правил (рисунок 2.6). Недолік: якщо пред'явити цим системам вкрадені ідентифікатор і секретний елемент (як правило, ім'я користувача і пароль), то і системи розмежування доступу, і міжмережеві екрани "пропустять" зломщика в корпоративну мережу

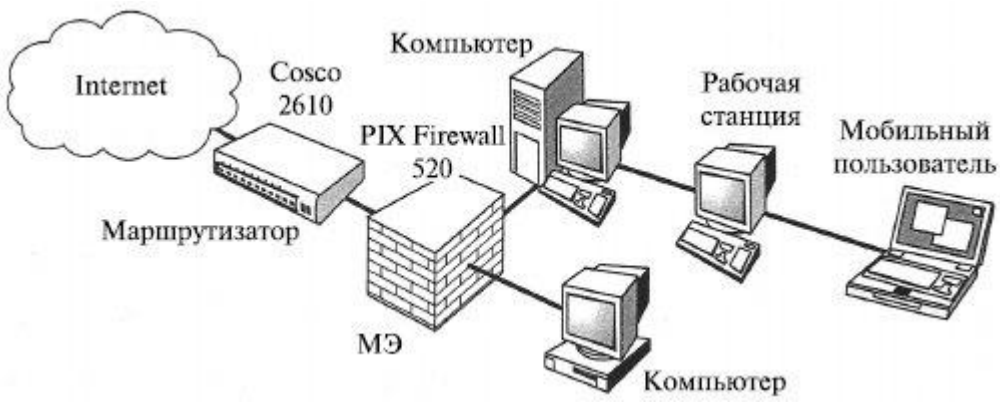


Рисунок 2.6 - Використання комплексу "маршрутизатор-фаєрвол" в системах захисту інформації при підключенні до Internet

Для усунення таких недоліків були розроблені нові технології і різні механізми захисту, з яких широке поширення одержали аналіз захищеності і виявлення атак. Найвідомішим продуктом в області аналізу захищеності є сімейство SAFEsuite американської компанії Internet Security Systems, яке складається з трьох систем, що виявляють уразливості ("дірки") і помилки в програмному забезпеченні - Internet Scanner, System Scanner і Database Scanner (рисунок 2.7).

Виявлення атак - це нова технологія, яка набула поширення в останні роки. Її відмінна особливість полягає у виявленні будь-яких атак, в тому числі вихідних і від авторизованих користувачів, і пропускаються міжмережевими екранами і засобами розмежування доступу. На цьому ринку також лідирує компанія ISS з системою виявлення атак RealSecure.

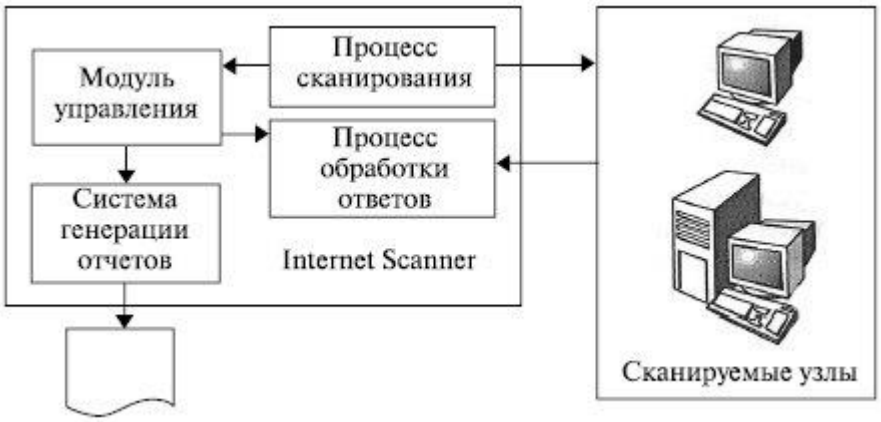


Рисунок 2.7 - Схема застосування скануючої системи інформаційної безпеки

Криптографія - це сукупність технічних, математичних, алгоритмічних і програмних методів перетворення даних (шифрування даних), яка робить їх марними для будь-якого користувача, у якого немає ключа для розшифровки.

Криптографічні перетворення забезпечують вирішення наступних базових завдань захисту - конфіденційності і цілісності.

Технології криптографії дозволяють реалізувати наступні процеси інформаційного захисту:

- ідентифікація (ототожнення) об'єкта або суб'єкта мережі або інформаційної системи;
- аутентифікація (перевірка дійсності) об'єкта або суб'єкта мережі;
- контроль / розмежування доступу до ресурсів локальної мережі або внесетевим сервісів;
- забезпечення та контроль цілісності даних.

Хто і як повинен займатися організацією захисту?

Питання визначення стратегії розробки, придбання і впровадження засобів захисту інформації, визначення кола першочергових задач і формування політики інформаційної безпеки є прерогативою вищого керівництва компанії. Питання реалізації та забезпечення ІБ прямо входять у сферу відповідальності керівника IT-департаменту (якщо компанія велика) або IT-відділу або IT-служби.

Стандартний набір засобів комплексного захисту інформації у складі сучасної ІС звичайно містить такі компоненти:

• засоби забезпечення надійного зберігання інформації з використанням технології захисту на файловому рівні (File Encryption System - FES);

• засоби авторизації і розмежування доступу до інформаційних ресурсів, а також захист від несанкціонованого доступу до інформації з використанням систем біометричної авторизації і технології токенів (смарт-карти, touch-memory, ключі для USB-портів і т.п.);

• засоби захисту від зовнішніх загроз при підключенні до загальнодоступних мереж зв'язку (Internet), а також засоби управління доступом в Internet з використанням технології міжмережевих екранів (Firewall) і змістовної фільтрації (Content Inspection);

• засоби захисту від вірусів з використанням спеціалізованих комплексів антивірусної профілактики;

• засоби забезпечення конфіденційності, цілісності, доступності та достовірності інформації, що передається по відкритих каналах зв'язку з використанням технології захищених віртуальних приватних мереж (VPN);

• засоби забезпечення активного дослідження захищеності інформаційних ресурсів з використанням технології виявлення атак (Intrusion Detection);

• засоби забезпечення централізованого управління системою інформаційної безпеки відповідно до узгодженої та затвердженої "Політикою безпеки компанії".

2.3 Розробка ключових методів системи захисту конфіденційної інформації

Як початкові об’єкти можуть застосовуватися алгебраїчні блокові коди з швидким (поліноміальної складності) алгоритмом декодування, такі, наприклад, як коди Гопи, Ріда – Соломона , Боуза – Чоудхурі – Хоквігнема . Найефективнішими за стійкістю до алгоритмів криптоаналізу є крипто-кодові засоби захисту інформації з недвійковими лінійними блоковими кодами, які виникають на алгебраїчних кривих – алгебро-геометричними кодами (АГК). З одного боку, подібні засоби стійкі до атак, запропонованих Сідєльніковим, з іншого боку, вони забезпечують високі показники достовірності і оперативності передавання даних. Водночас практичне використання крипто-кодових засобів захисту інформації з недвійковими алгебраїчними блоковими кодами передбачає застосування методів і обчислювальних алгоритмів недвійкового рівновагового кодування (як за схемою Мак – Еліса, так і за схемою Нідеррайтера). На сьогодні існуючий науково-методичний апарат, застосовувані методи і обчислювальні алгоритми не дозволяють реалізувати недвійкове рівновагове кодування, в тому числі і в крипто-кодових засобах захисту інформації. Отже, актуальним науково-технічним завданням, що має важливе прикладне значення в ділянці побудови обчислювально ефективних криптографічних засобів захисту інформації, є розроблення методів і алгоритмів недвійкового рівновагового кодування і крипто-кодових засобів на їх основі для комплексного забезпечення безпеки і достовірності передавання даних у КСіМ.

Структура побудови показника така, що в ній об’єднано дві основні характеристики системи: необхідна ймовірність досягнення мети забезпечення конфіденційності (інформаційної прихованості) в певних умовах зовнішнього середовища і при певному рівні впливу внутрішніх випадкових чинників та витрати, які необхідно провести у вказаних умовах для досягнення мети з необхідною ймовірністю. Цей показник, включаючи характеристики достовірності, конфіденційності і часу отримання даних в комп’ютерній мережі (КМ), по суті, відбиває швидкість достовірного і конфіденційного передавання даних, що дає змогу оцінювати ефективність мережі в широкому діапазоні

інтенсивностей помилок в каналі передавання даних при різних швидкостях передавання *R*:

$$W(u_i) = \frac{n\left(t^{u_i}\right)-1}{n\left(t^{u_i}\right)} \cdot \frac{B^{(u_i)} - \psi^{(u_i)}}{B^{(u_i)}} \cdot P_{np.n}^{u_i} \qquad (2.1)$$

де $W(u_i)$ – показник ефективності КМ при обраній стратегії (методі підвищення достовірності) u_i ; $n^{(ui)}$ – число інформаційних розрядів пакету при обраній стратегії u_i за даний час; $t^{(ui)}$ – час доставки пакету *t* при вибраній стратегії u_i ;

$B^{(ui)}$ – кількість операцій, необхідних для розкриття криптоалгоритму порушником при обраній стратегії u_i ; $\Psi^{(ui)}$ – кількість операцій обчислювальної системи, доступної криптоаналітику (противнику) при обраній стратегії u_i ; $P_{np\,n}{}^{(ui)}$ – ймовірність правильної доставки пакету при обраній стратегії; *U* – більшість допустимих стратегій (методів підвищення достовірності, які використовуються в КМ). При цьому окремі характеристики повинні задовольняти систему обмежень $\left\{T_Б \geq T_Д, P_{пом} \leq P_Д, t_д \leq t_Д\right\}$, при мінімізації часу доставки кадру інформації де: *ТБ* – безпечний час роботи криптоалгоритму; $T_Д$ - допустимий безпечний час, $T_Д \leq 200$ років при передаванні конфіденційної інформації комерційними каналами зв'язку; *P* – ймовірність помилкового приймання; $P_Д$ - допустима ймовірність помилкового приймання символів повідомлення, становить $P_Д < 10^{-7} – 10^{-9}$ в залежності від категорії цінності інформації, яка опрацьовується, її пріоритетності і належності; $t_д$ – час приймання пакету; $t_Д$ - допустимий час приймання пакету, складає $t_Д \leq 10^{-3} – 10^{-9}$ *с* в залежності від вибраної стратегії підвищення достовірності передавання повідомлень.

Узагальнений показник ефективності КМ повинен мати значення $W(u_i) \geq 0{,}9$ при заданих критеріях ефективності КМ. Обрані узагальнений показник і критерій дозволяють отримати числові значення, які характеризують швидкість достовірного і конфіденційного передавання даних в КМ і здійснити порівняння

існуючих протоколів ГОС за ефективністю обміну даними між двома вузлами КМ.

Розглянуто формальний математичний опис крипто-кодових засобів захисту інформації, досліджено процес крипто-кодового перетворення інформації і передавання даних у режимі автоматичного перезапиту. Введено формальне математичне визначення крипто-кодових засобів захисту інформації з використанням недвійкових рівновагових кодів та запропоновано обчислювальні алгоритми перетворення інформації.

Формальне математичне визначення крипто-кодової системи захисту інформації на недвійкових рівновагових кодах і з використанням алгебраїчних блокових кодів в режимі виявлення помилок і автоматичного перезапиту введено так:

– множина відкритих текстів

$$M = (M_1, M_2, ..., M_{q^m}), \text{ де } M_i = (I_0, I_1, ..., I_{m-1}),\ \forall I_j \in GF(q) \tag{2.2}$$

причому кожному M_i можна однозначно співставити вектор

$$\varepsilon_i = (e_0, e_1, ..., e_{n-1}),\ \forall e_j \in GF(q),\ w(\varepsilon_i) \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor \tag{2.3}$$

з множини $\Phi = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_{q^m})$, тобто, виконується відображення $\psi : M \to \Phi$

так, що для $\forall i$ справедливо $\varepsilon_i = \psi(M_i)$, де Ψ задається процедурою недвійкового (за основою q) рівновагового кодування;

– множина криптограм $E = (E_1, E_2, ..., E_{q^m})$ (2.4)

де $E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}})$, $\forall S_{X_j} \in GF(q)$, причому кожному E_i можна однозначно співставити вектор ε_i;

– множина прямих відображень $\varphi = \{\varphi_1, \varphi_2, ..., \varphi_s\}$ (2.5)

де φ_j: $M \to E$, $j = 1, 2, ..., s$, причому для $\forall j$ справедливо $E_i = \varphi_j(m_i)$;

– множина зворотних відображень $\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1}\}$ (2.6)

де φ_j^{-1}: $E \to M$, $j = 1, 2, ..., s$, причому для $\forall j$ справедливо $m_i = \varphi_j^{-1}(E_i)$;

– множина ключів, які параметризують прямі відображення:

$$K = \{K_1, K_2, ..., K_s\} = \{H_X^1, H_X^2, ..., H_X^s\} \quad (2.7)$$

тобто $\varphi_j : M \xrightarrow{K_j} E$, $E_i = \varphi_j(m_i, K_j)$;

– множина ключів, які параметризують зворотні відображення

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\} \quad (2.8)$$

тобто $\varphi_j^{-1} : E \xrightarrow{K_j^*} M$, $m_i = \varphi_j^{-1}(E_i, K_j^*)$. Виконання зворотного відображення φ^{-1}, тобто обчислення $m_i = \varphi_j^{-1}(E_i)$ без знання ключа

$$K_j^* \in K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\}$$

пов'язана з розв'язанням теоретико–складної задачі декодування випадкового коду (коду загального положення). Множини M, Φ, і E рівнопотужні, тобто

$$|M| = |\Phi| = |E| = q^m \quad (2.9)$$

причому потужність q^m не перевищує потужності рівновагового коду, тобто повної множини послідовностей довжини n і ваги $w(\varepsilon_i)$: $q^m \le C_n^{w(\varepsilon_i)}$ (10),

звідки маємо: $m \le log_q\left(C_n^{w(\varepsilon_i)}\right)$.

Початковими даними при описі розглянутої несиметричної крипто–кодової системи захисту інформації є:

– недвійковий рівноваговий код над *GF(q)*, тобто множина послідовностей довжини n і ваги $w(\varepsilon_i)$;

– недвійковий алгебраїчний блоковий *(n, k, d)* код C над *GF(q)*, тобто множина кодових слів $C_i \in C$ таких, що виконується рівняння $C_i H^T = 0$, де H – перевірочна матриця алгебраїчного блокового коду;

– маскувальні матричні відображення, задані множиною матриць $\{X,P,D\}_i$, де X – невироджена $k \times k$ матриця над *GF(q)*, P – перестановочна $n \times n$ матриця над *GF(q)* з одним ненульовим елементом в кожному рядку і в кожному стовпчику матриці, D – діагональна $n \times n$ матриця над *GF(q)* з ненульовими елементами на головній діагоналі.

На рисунку 2.8 схематично зображено основні етапи формування криптограми з вказанням методів кодування, які застосовуються. Схему процесу зворотного крипто-кодового перетворення в режимі виявлення помилок і автоматичного перезапиту подано на рисунок 2.9.

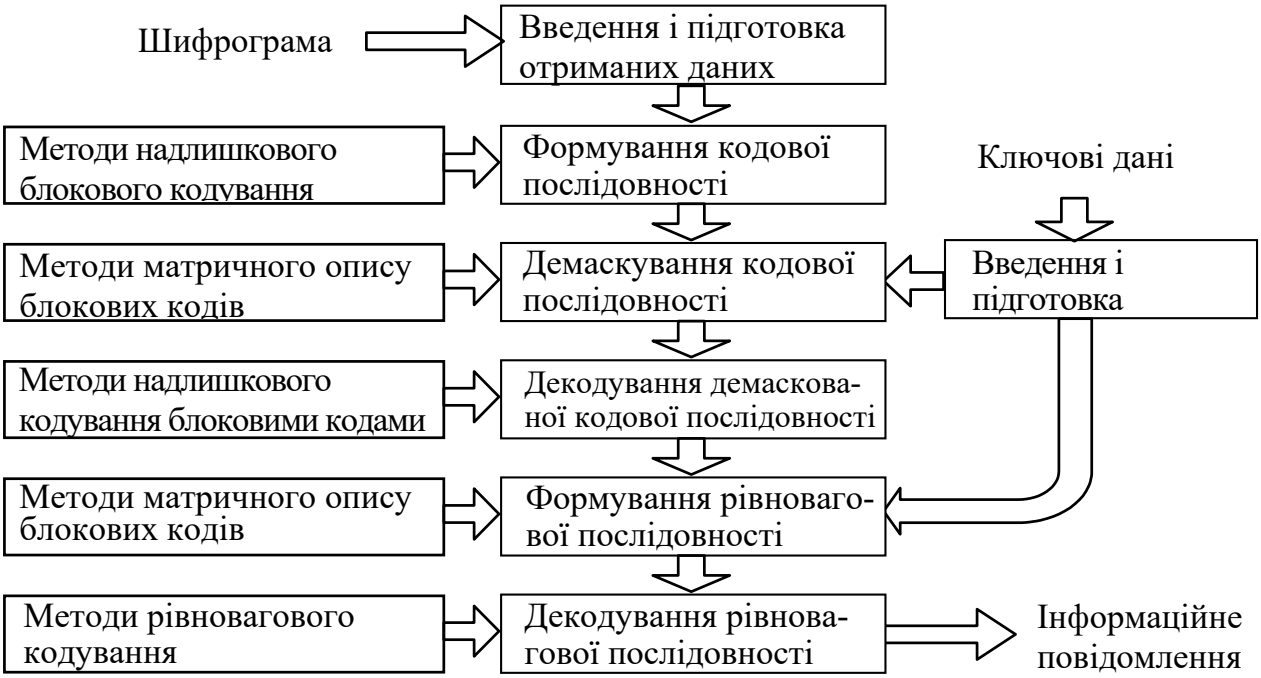


Рисунок 2.9 - Схема процесу зворотного крипто-кодового перетворення

Висновки до розділу 2

Розвиток підходів до рішення проблеми захисту інформації проходив від забезпечення захисту лише формальними механізмами, що містять головним чином технічні й програмні засоби в рамках ОС і СУБД, через виділення керуючого компонента, ядра безпеки, і розвиток неформальних засобів захисту до формування погляду на захист як на неперервний процес, до розвитку стандартів, посиленню тенденції апаратної реалізації функцій захисту, формуванню висновку про взаємозв'язок захисту інформації, архітектури систем обробки даних і технології їх функціонування, до формування *системного комплексного підходу*, що є визначальним на сучасному етапі розвитку.

Необхідно захищатися від:

• від порушення інформаційних каналів і ресурсів;

• від несанкціонованого доступу до інформації, що приводить до порушення її цілісності;

• від руйнування засобів захисту що вбудовані, призначених для доказу неправомірних дій користувачів і обслуговуючого персоналу;

• від впровадження "вірусів" і "закладок" в програмні продукти та технічні засоби.

Умовно можна виділити три категорії засобів захисту - традиційні засоби, нові технології та засоби криптографічного захисту інформації.

Технології криптографії дозволяють реалізувати наступні процеси інформаційного захисту:

• ідентифікація (ототожнення) об'єкта або суб'єкта мережі або інформаційної системи;

• аутентифікація (перевірка дійсності) об'єкта або суб'єкта мережі;

• контроль / розмежування доступу до ресурсів локальної мережі або внесетевим сервісів;

• забезпечення та контроль цілісності даних.

3 РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ПРИВАТНИХ ОРГАНІЗАЦІЯХ

3.1 Реалізація системи захисту конфіденційної інформації

Запропонований метод заснований на представленні інформаційних даних у вигляді числового еквіваленту A з подальшим розкладанням в лінійну комбінацію біноміальних коефіцієнтів, кожен з яких кодується позиційною нумерацією так, щоб виконувалася система кодових обмежень за довжиною рівновагових послідовностей n, ваги кодових слів w і потужності коду

$$M:\ \forall j: w(C_j) = const = w;\ 0 \le A < M;\ 0 \le w \le n;\ 0 \le C_{ji} < q.$$

Число A подано у вигляді рівновагової недвійкової послідовності

$C_A = (C_{A_0} \quad C_{A_1} \quad \dots \quad C_{A_{n-1}})$, причому $A = \mathrm{A_Б} \cdot (\mathrm{q}-1)^w + A_П$, де $A_Б = \sum_{i=0}^{n-1} a_{Бi} b_i$,

$b_i = \binom{n-i-1}{w-l}$, $A_П = \sum_{l=0}^{w-1} (a_l - 1) h^l$, $h = q - 1$.

Запропонована система обчислення на основі узагальненого біноміально-позиційного представлення чисел заснована на комплексному використанні системи біноміального рахунку (через зростаючу послідовність біноміальних коефіцієнтів задається розміщення ненульових елементів) і позиційної системи обчислення (значення ненульових елементів задають через помісне значення чисел). Застосування розробленої системи забезпечує побудову ефективних методів недвійкового рівновагового кодування та їх практичного використання.

Запропонований алгоритм недвійкового рівновагового кодування, заснований на запропонованому методі, перетворить число A на рівновагову недвійкову послідовність $C_A = (C_{A_0} \quad C_{A_1} \quad \dots \quad C_{A_{n-1}})$ і складається з наступних кроків:

1. Ввести параметри, n, w, q і число $A < M$, яке належить недвійковому рівноваговому кодуванню.

2. Представити число A у вигляді $A = \mathrm{A}_{\mathrm{Б}} \cdot (\mathrm{q}-1)^w + A_{П}$, тобто обчислити:

2.1. $A_{Б} = \left\lfloor \frac{A}{(\mathrm{q}-1)^w} \right\rfloor$;

2.2. $A_{П} = (A) \bmod ((\mathrm{q}-1)^w)$.

3. Закодувати число $A_{Б}$ двійковим біноміальним кодом:

3.1. Прийняти $x = A_{Б}$, $i = 0$, $l = 0$;

3.2. Обчислити число $b_i = \binom{n-i-1}{w-l}$;

3.3. Якщо $b_i > x$:

3.3.1. $a_{Б_{n-i-1}} = 0$;

3.3.2. $i = i + 1$ і перейти до кроку 3.2.

3.4. Якщо $b_i \le x$:

3.4.1. $a_{Б_{n-i-1}} = 1$;

3.4.2. $x = x - b_i$;

3.4.3. $i = i + 1$;

3.4.4. $l = l + 1$ і перейти до кроку 3.2.

3.5. Сформувати вектор $(a_{Б0} \quad a_{Б1} \quad \ldots \quad a_{Бn-1})$.

4. Закодувати число $A_{П}$ позиційним кодом довжини w за основою $q-1$:

4.1. Прийняти $x = A_{П}$, $l = 0$;

4.2. Обчислити $a_l = (x) \bmod (q-1) + 1$;

4.3. Обчислити $x = \left\lfloor \frac{x}{q-1} \right\rfloor$;

4.4. $l = l + 1$;

4.5. Якщо $l < w$ перейти до 4.2;

4.6. Сформувати вектор $(a_0 \quad a_1 \quad \ldots \quad a_{w-1})$.

5. Сформувати недвійкову рівновагову послідовність:

5.1. Прийняти $i = 0$, $l = 0$.

5.2. Якщо $a_{Б_i} \neq 0$:

5.2.1. $C_{A_i} = a_l$;

5.2.2. $l = l + 1$;

5.2.3. $i = i + 1$ і перейти до кроку 5.2.

5.3. Якщо $a_{Б_i} = 0$:

5.3.1. $C_{A_i} = 0$;

5.3.2. $i = i + 1$ і перейти до кроку 5.2.

5.4. Сформувати вектор $\left(C_{A_0} \quad C_{A_1} \quad ... \quad C_{A_{n-1}}\right)$.

6. Вивести вектор $C_A = \left(C_{A_0} \quad C_{A_1} \quad ... \quad C_{A_{n-1}}\right)$.

Отже, запропонований алгоритм формування недвійкових рівновагових послідовностей реалізується через сукупність простих і обчислювально ефективних перетворень, заснованих на елементарних двійкових операціях над елементами послідовностей. З погляду практичної реалізації розробленого методу і алгоритмів недвійкового рівновагового кодування найбільш доцільним є застосування недорогих обчислювальних пристроїв на базі ПЛІС і СМАРТ-карт. Формування криптограм у запропонованих крипто-кодових засобах захисту інформації здійснюють за допомогою виконання процедур і функцій рівновагового і нерівновагового алгебраїчного кодування, методів маскування відповідних кодів під випадкову послідовність і функціональних операцій над кінцевими полями.

3.2 Тестування системи захисту конфіденційної інформації

У процесі подальших досліджень побудовано цикли криптоперетворення представлені на рисунку 3.1, які стали основою побудови орієнтованого псевдографа криптографічних перетворень, представленого на рисунку 3.2.

Таблиця 3.1 - Матричні моделі криптографічного перетворення відібрані для обчислювального експерименту

Кодування	Розкодування	Кодування	Розкодування
$M_1^k = F_{3,5}^k = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$	$M_1^d = F_{3,5}^d = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$	$M_4^k = F_{5,3}^k = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$	$M_4^d = F_{5,3}^d = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
$M_2^k = F_{6,5}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$	$M_2^d = F_{6,5}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$	$M_5^k = F_{5,6}^k = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}$	$M_5^d = F_{5,6}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$
$M_3^k = F_{3,6}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix}$	$M_3^d = F_{3,6}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix}$	$M_6^k = F_{6,3}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$	$M_6^d = F_{5,6}^d = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}$

Таблиця 3.2 - Результати обчислювального експерименту (№1)

	M_1^k	M_2^k	M_3^k	M_4^k	M_5^k	M_6^k
$O_1^{\oplus}$	$O_1^{\oplus}$ M_1^k	$O_1^{\oplus}$ M_2^k	$O_1^{\oplus}$ M_3^k	$O_1^{\oplus}$ M_4^k	$O_1^{\oplus}$ M_6^k	$O_1^{\oplus}$ M_5^k
$O_2^{\oplus}$	$O_1^{\oplus}$ M_1^k	$O_2^{\oplus}$ M_2^k	$O_4^{\oplus}$ M_3^k	$O_2^{\oplus}$ M_4^k	$O_3^{\oplus}$ M_6^k	$O_4^{\oplus}$ M_5^k
$O_3^{\oplus}$	$O_1^{\oplus}$ M_1^k	$O_4^{\oplus}$ M_2^k	$O_3^{\oplus}$ M_3^k	$O_3^{\oplus}$ M_4^k	$O_4^{\oplus}$ M_6^k	$O_2^{\oplus}$ M_5^k
$O_4^{\oplus}$	$O_1^{\oplus}$ M_1^k	$O_3^{\oplus}$ M_2^k	$O_2^{\oplus}$ M_3^k	$O_4^{\oplus}$ M_4^k	$O_2^{\oplus}$ M_6^k	$O_3^{\oplus}$ M_5^k
$O_5^{\oplus}$	$O_1^{\oplus}$ M_1^k	---- -----	---- -----	$O_5^{\oplus}$ M_4^k	---- -----	---- -----

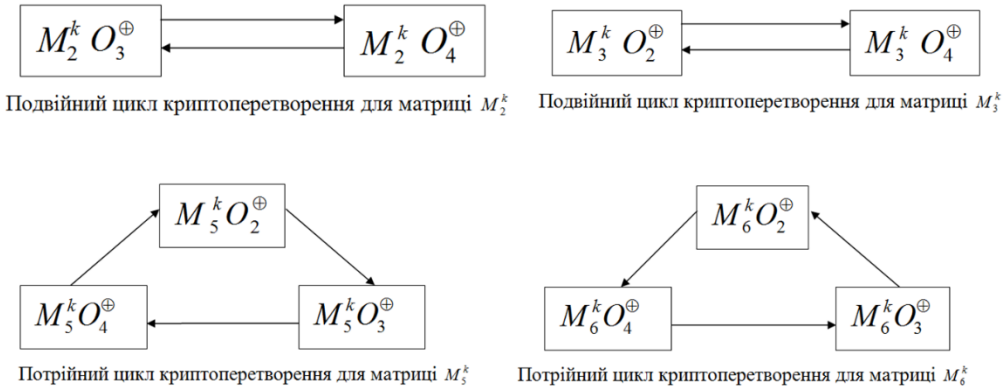


Рисунок 3.1 - Цикли криптоперетворення

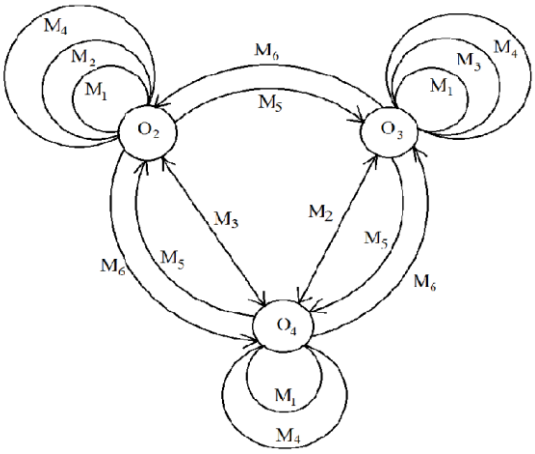


Рисунок 3.2 - Орієнтований псевдограф криптоперетворень на основі матричних алгоритмів, що досліджуються

Результати аналізу орієнтованого псевдографу криптографічних перетворень на основі матричних алгоритмів (таблиця 3.3) підтверджують результати теоретичних досліджень.

Таблиця 3.3 - Результати аналізу орієнтованого псевдографу криптографічних перетворень на основі матричних алгоритмів, що досліджуються

Повне симетричне крипто-перетворення	M_1^k	$O_2^{\oplus} \to O_2^{\oplus}$ $O_3^{\oplus} \to O_3^{\oplus}$ $O_4^{\oplus} \to O_4^{\oplus}$	0-арна дія	Моноцикли
	M_4^k		унарна дія	
Частково несиметричне крипто-перетворення	M_2^k	$O_2^{\oplus} \to O_2^{\oplus}$	0-арна дія з правою підстановкою	Моноцикл + Подвійний цикл
		$O_3^{\oplus} \to O_4^{\oplus} \to O_3^{\oplus}$		
	M_3^k	$O_3^{\oplus} \to O_3^{\oplus}$	0-арна дія з лівою підстановкою	
		$O_2^{\oplus} \to O_4^{\oplus} \to O_2^{\oplus}$		
Повне несиметричне крипто-перетворення	M_5^k	$O_2^{\oplus} \to O_3^{\oplus} \to O_4^{\oplus} \to O_2^{\oplus}$	унарна дія з правою підстановкою	Потрійний цикл
	M_6^k	$O_2^{\oplus} \to O_4^{\oplus} \to O_3^{\oplus} \to O_2^{\oplus}$	унарна дія з лівою підстановкою	

Результати подальших досліджень надали змогу формалізувати встановлені взаємозв’язки між матричними алгоритмами та синтезованими операціями при їх взаємному використанні в криптографічних перетвореннях та довести їх коректність, що забезпечило можливість побудови моделі синтезу операції оберненого матричного криптографічного перетворення.

Запропоновано метод синтезу та технологію дослідження операцій додавання за модулем два з точністю до перестановки результатів виконання операції, яка забезпечує синтез модифікованих операцій, придатних для криптографічних перетворень, та уніфікує процес знаходження взаємозв’язків

між матричними алгоритмами та синтезованими модифікованими операціями при їх взаємному використанні в криптографічних перетвореннях.

Узагальнена таблична форма представлення операції $O_1^{\oplus}$ наведена в таблиці 3.4.

Для формалізації отриманих результатів досліджень введемо наступні позначення: $P^{op}_{(0123)}$ – перестановка операндів операції, де (0123) – варіант перестановки операндів; $P^{ro}_{(1023)}$ – перестановка результатів виконання операції; $P^{op}_{(0123)}(O_1^{\oplus})$ – перестановка операндів операції $O_1^{\oplus}$; $P^{ro}_{(1023)}(O_4^{\oplus})$ – перестановка результатів виконання операції $O_4^{\oplus}$.

Таблиця 3.4 - Узагальнена таблична форма представлення операції $O_1^{\oplus}$

$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$		**0**	**1**	**2**	**3**
	0	**0**	**1**	**2**	**3**
	1	**1**	**0**	**3**	**2**
	2	**2**	**3**	**0**	**1**
	3	**3**	**2**	**1**	**0**
		0	**1**	**2**	**3**
	0	**a**	**b**	**c**	**d**
	1	**b**	**a**	**d**	**c**
	2	**c**	**d**	**a**	**b**
	3	**d**	**c**	**b**	**a**

Як видно з таблиці 3.5, лише чотири варіанти перестановок операції $O_1^{\oplus}$ можуть бути використані для реалізації операцій криптографічного перетворення інформації: це перестановки $P^{op}_{(0123)}(O_1^{\oplus})$, $P^{op}_{(1032)}(O_1^{\oplus})$, $P^{op}_{(2301)}(O_1^{\oplus})$, $P^{op}_{(3210)}(O_1^{\oplus})$.

Таблиця 3.5 - Експериментальні дані щодо використання операції з точністю до перестановки результатів

$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$	**Перестановка**		**Перестановка**		**Перестановка**		**Перестановка**	
	1	**0 1 2 3**	**7**	1 0 2 3	**13**	2 1 0 3	**19**	3 1 2 0
	2	0 1 3 2	**8**	**1 0 3 2**	**14**	2 1 3 0	**20**	3 1 0 2
	3	0 2 3 1	**9**	1 2 3 0	**15**	2 0 3 1	**21**	3 2 0 1
	4	0 2 1 3	**10**	1 2 0 3	**16**	2 0 1 3	**22**	**3 2 1 0**
	5	0 3 1 2	**11**	1 3 0 2	**17**	2 3 1 0	**23**	3 0 1 2
	6	0 3 2 1	**12**	1 3 2 0	**18**	**2 3 0 1**	**24**	3 0 2 1

Побудовано перестановочні схеми синтезу модифікованих операцій та перевірено коректність отриманих результатів. Аналогічно досліджені інші синтезовані операції додавання за модулем два з точністю до перестановки результатів виконання операцій. Отримані результати досліджень наведено в таблиці 3.6.

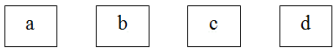
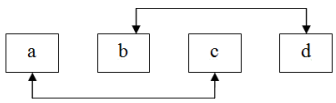
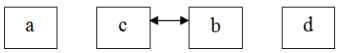
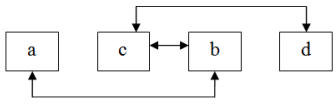
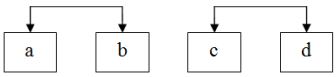
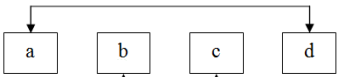
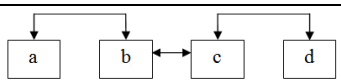
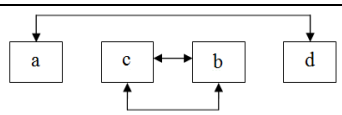
Необхідно зауважити, що варіанти перестановок, на основі яких побудовані модифікації операцій $O_1^{\oplus}$ і $O_3^{\oplus}$, співпадають. Аналогічно співпадають і варіанти перестановок для побудови модифікацій операцій $O_2^{\oplus}$ і $O_4^{\oplus}$.

Для візуалізації результатів дослідження побудовано узагальнені перестановочні схеми для синтезу операцій на основі перестановки результатів, які наведено в таблиці 3.7.

Таблиця 3.6 - Модифікації операцій $O_1^{\oplus}$ - $O_4^{\oplus}$ придатні для криптографічного перетворення

	Перестановка 1	Перестановка 2	Перестановка 3	Перестановка 4
$O_1^{\oplus} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$	a b c d	b a d c	c d a b	d c b a
	$P^{op}_{(0123)}(O_1^{\oplus})$	$P^{op}_{(1032)}(O_1^{\oplus})$	$P^{op}_{(2301)}(O_1^{\oplus})$	$P^{op}_{(3210)}(O_1^{\oplus})$
$O_2^{\oplus} = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix}$	a c b d	b d a c	c a d b	d b c a
	$P^{op}_{(0213)}(O_2^{\oplus})$	$P^{op}_{(1302)}(O_2^{\oplus})$	$P^{op}_{(2031)}(O_2^{\oplus})$	$P^{op}_{(3120)}(O_2^{\oplus})$
$O_3^{\oplus} = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}$	a b c d	b a d c	c d a b	d c b a
	$P^{op}_{(0123)}(O_3^{\oplus})$	$P^{op}_{(1032)}(O_3^{\oplus})$	$P^{op}_{(2301)}(O_3^{\oplus})$	$P^{op}_{(3210)}(O_3^{\oplus})$
$O_4^{\oplus} = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}$	a c b d	b d a c	c a d b	d b c a
	$P^{op}_{(0213)}(O_4^{\oplus})$	$P^{op}_{(1302)}(O_4^{\oplus})$	$P^{op}_{(2031)}(O_4^{\oplus})$	$P^{op}_{(3120)}(O_4^{\oplus})$

Таблиця 3.7 - Узагальнені перестановочні схеми результатів виконання операцій для їх модифікації

№ перестановки	Операція	Перестановочна схема	№ перестановки	Операція	Перестановочна схема
1	$O_1^{\oplus}$ і $O_3^{\oplus}$		3	$O_1^{\oplus}$ і $O_3^{\oplus}$	
	$O_2^{\oplus}$ і $O_4^{\oplus}$			$O_2^{\oplus}$ і $O_4^{\oplus}$	
2	$O_1^{\oplus}$ і $O_3^{\oplus}$		4	$O_1^{\oplus}$ і $O_3^{\oplus}$	
	$O_2^{\oplus}$ і $O_4^{\oplus}$			$O_2^{\oplus}$ і $O_4^{\oplus}$	

За результатами дослідження встановлено, що всі 16 модифікованих операцій на основі операції додавання за модулем два, які складають повну групу даних операцій, можна отримати за допомогою поєднання трьох попарних перестановок та однієї одинарної перестановки результатів виконання операцій.

Як і в другому розділі, було проведено дослідження повної групи синтезованих операцій за модулем два з точністю до перестановки.

Результати аналізу криптоперетворень на основі матричних алгоритмів показали, що всі синтезовані операції мають однакову арність і є унарними. Крім того слід зазначити, що всі зазначені операції побудовані на базі однієї операції додавання за модулем два шляхом перестановки операндів та результатів виконання операції і мають однакові властивості.

Математичні моделі даних операцій можна представити наступним чином:

$$P^{op}_{(0123)}(O^{\oplus}_1)=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\end{vmatrix};\qquad P^{op}_{(1032)}(O^{\oplus}_1)=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix};\qquad P^{op}_{(2301)}(O^{\oplus}_1)=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\end{vmatrix};$$

$$P^{op}_{(3210)}(O^{\oplus}_1)=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix};$$

$$P^{op}_{(0213)}(O^{\oplus}_2)=\begin{vmatrix} x_{1.1}\oplus x_{2.2} \\ x_{1.2}\oplus x_{2.1}\end{vmatrix};\qquad P^{op}_{(1302)}(O^{\oplus}_2)=\begin{vmatrix} x_{1.1}\oplus x_{2.2} \\ x_{1.2}\oplus x_{2.1}\oplus 1\end{vmatrix};\qquad P^{op}_{(2031)}(O^{\oplus}_2)=\begin{vmatrix} x_{1.1}\oplus x_{2.2}\oplus 1 \\ x_{1.2}\oplus x_{2.1}\end{vmatrix};$$

$$P^{op}_{(3120)}(O^{\oplus}_2)=\begin{vmatrix} x_{1.1}\oplus x_{2.2}\oplus 1 \\ x_{1.2}\oplus x_{2.1}\oplus 1\end{vmatrix}$$

$$P^{op}_{(0123)}(O^{\oplus}_3)=\begin{vmatrix} x_{1.2}\oplus x_{2.1} \\ x_{1.1}\oplus x_{2.2}\end{vmatrix};\qquad P^{op}_{(1032)}(O^{\oplus}_3)=\begin{vmatrix} x_{1.2}\oplus x_{2.1} \\ x_{1.1}\oplus x_{2.2}\oplus 1\end{vmatrix};\qquad P^{op}_{(2301)}(O^{\oplus}_3)=\begin{vmatrix} x_{1.2}\oplus x_{2.1}\oplus 1 \\ x_{1.1}\oplus x_{2.2}\end{vmatrix};$$

$$P^{op}_{(3210)}(O^{\oplus}_3)=\begin{vmatrix} x_{1.2}\oplus x_{2.1}\oplus 1 \\ x_{1.1}\oplus x_{2.2}\oplus 1\end{vmatrix}$$

$$P^{ro}_{(0213)}(O^{\oplus}_4)=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\end{vmatrix};\qquad P^{ro}_{(1302)}(O^{\oplus}_4)=\begin{vmatrix} x_{1.1}\oplus x_{2.1} \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix};\qquad P^{ro}_{(2031)}(O^{\oplus}_4)=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\end{vmatrix};$$

$$P^{ro}_{(3120)}(O^{\oplus}_4)=\begin{vmatrix} x_{1.1}\oplus x_{2.1}\oplus 1 \\ x_{1.2}\oplus x_{2.2}\oplus 1\end{vmatrix};$$

Схема реалізації наведеної групи операцій подана на рисунку 3.3. Застосування цієї схеми для потокового шифрування наведено на рисунку 3.4.

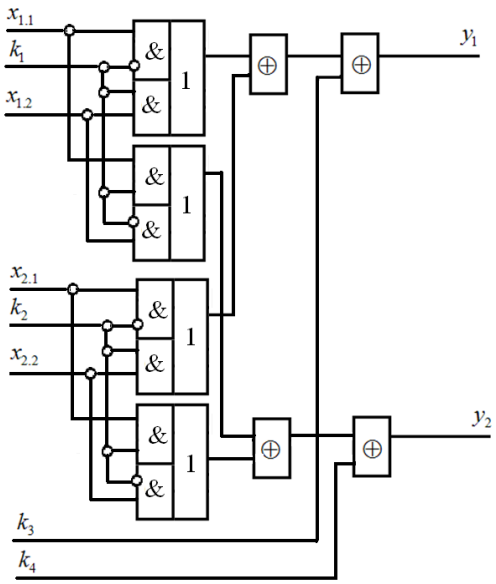


Рисунок 3.3 - Універсальна схема реалізації групи операцій додавання за модулем два з точністю до перестановки

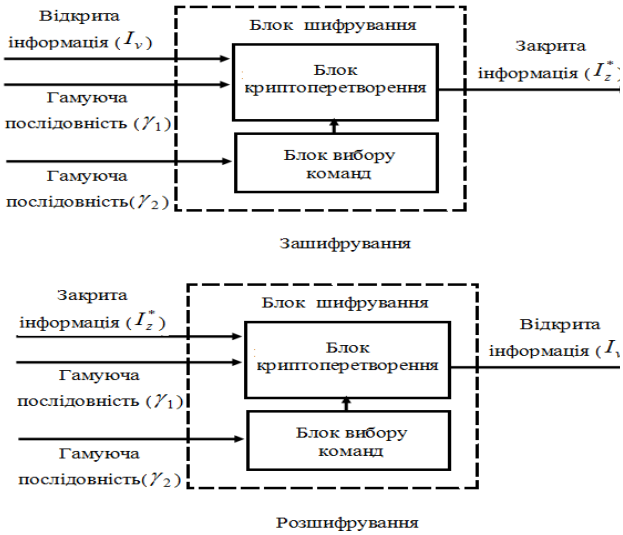


Рисунок 3.4 - Структурна схема потокового шифрування з використанням групи модифікованих операцій криптографічного додавання за модулем два
з точністю до перестановки

Для перевірки коректності гіпотези, що всі модифікації операцій мають однакові криптографічні властивості, проведено оцінку статистичних властивостей результатів шифрування з використанням пакету NIST_STS. Результати кількісної оцінки результатів тестування шифрування наведено в таблиці 3.8.

Як видно зі зведених результатів, досліджувані послідовності пройшли комплексний контроль за методикою випробувань пакетом тестів NIST_STS. Слід відмітити, що якість отриманої псевдовипадкової послідовності при використанні повної групи модифікацій операцій найкраща з повної множини розглянутих прикладів.

Таблиця 3.8 - Зведена таблиця тестування результатів шифрування

Кількість тестів, у	**Шифрування випадковими матричними алгоритмами**

яких тестування пройшли більш ніж	**з використанням:**		
	Однієї операції	Чотирьох модифікацій операцій	Повної групи модифікацій операцій
100 % послідовностей	65 (35 %)	65 (35 %)	69 (37%)
99 % послідовностей	127 (68 %)	128 (68 %)	131 (70%)
98 % послідовностей	172 (91 %)	171 (91 %)	172 (91%)
97 % послідовностей	180 (96 %)	181 (96 %)	185 (98 %)
96 % послідовностей	188 (100 %)	188 (100 %)	188 (100 %)

Проведемо оцінку результатів порівняльного аналізу. Нехай подія A – наявність відкритої вхідної інформації, B – наявність першої гамуючої послідовності, C – наявність другої гамуючої послідовності, D – правильне функціонування пристрою; D_+ – правильне функціонування пристрою з покращеною якістю шифрування; H – на виході зашифрована гамуюча послідовність; G – передумова до зламу ключа; F – передумови витоку інформації чи зламу ключа; W – передумова витоку інформації.

Відповідно до таблиці 3.9, за умови рівномірного розподілу подій, отримаємо:

$$P_D(ABC) = \frac{3}{8} > P_D(AB) = \frac{1}{4};\ P_{D_+}(ABC) = \frac{1}{8} > P_{D_+}(AB) = 0;\ P_W(ABC) = \frac{1}{8} < P_W(AB) = \frac{1}{4};$$

$$P_G(ABC) = \frac{2}{8} = P_G(AB) = \frac{1}{4};\qquad P_H(ABC) = \frac{1}{8} > P_H(AB) = 0;\qquad P_F(ABC) = \frac{3}{8} < P_F(AB) = \frac{2}{4}$$

Таблиця 3.9 - Взаємозв’язки між вхідними і вихідними подіями

Потокове шифрування	**Вхідні події**	**Вихідні події**						
		D	$\overline{D}$	D_+	W	H	G	F
З використанням однієї операції	$A\,B$	+	–		–		–	
	$A\,\overline{B}$	–	+		+		–	+
	$\overline{A}\,B$	–	+		–		+	+
	$\overline{A}\,\overline{B}$	–	+		–		–	
З використанням групи операцій	$A\,B\,C$	+	–	+	–	–	–	–
	$A\,B\,\overline{C}$	+	–	–	–	–	–	–
	$A\,\overline{B}\,C$	+	–	–	–	–	–	–
	$\overline{A}\,B\,C$	–	+	–	–	+	–	–
	$A\,\overline{B}\,\overline{C}$	–	+	–	+	–	–	+
	$\overline{A}\,B\,\overline{C}$	–	+	–	–	–	+	+
	$\overline{A}\,\overline{B}\,C$	–	+	–	–	–	+	+
	$\overline{A}\,\overline{B}\,\overline{C}$	–	+	–	–	–	–	–

За умови однократної відмови (однієї оберненої вхідної події) отримаємо:

$$P_D^*(ABC)=\frac{3}{4}>P_D^*(AB)=\frac{1}{3};\quad P_{D_+}^*(ABC)=\frac{1}{4}>P_{D_+}^*(AB)=0;\quad P_W^*(ABC)=0<P_W^*(AB)=\frac{1}{3};$$

$$P_G^*(ABC)=0<P_G^*(AB)=\frac{1}{3};\quad P_H^*(ABC)=\frac{1}{4}>P_H^*(AB)=0;\quad P_F^*(ABC)=0<P_F^*(AB)=\frac{1}{2}.$$

Ймовірність правильного функціонування запропонованої схеми буде більшою на 1/8, що забезпечить збільшення надійності до 12,5 %, а при обмеженні на одну відмову буде більшою на 5/12, що забезпечить збільшення надійності до 41,6 %.

За результатами порівняння можна зробити висновок, що використання групи операцій додавання за модулем два з точністю перестановки на основі

додаткової гамуючої послідовності забезпечить підвищення якості шифрування і надійності роботи, а при однократних відмовах каналів вхідної інформації – виключить можливість створення передумови витоку інформації чи зламу ключа.

Отримані результати дозволяють сформулювати метод підвищення стійкості і надійності потокового шифрування, який полягає у виборі для кожного етапу шифрування модифікацій операції за модулем два з точністю до перестановки на основі додаткової гамуючої послідовності, що виключить при однократних відмовах можливість витоку інформації чи спрощення зламу ключа.

Дослідження можливості встановлення залежності між вхідною інформацією і результатами шифрування та можливість встановлення залежності в зашифрованій гамуючій послідовності з використанням математичного апарату мінімізації недетермінованих кінцевих автоматів, а саме: алгоритму кластеризації ситуацій для застосування незакінченого методу застосування гілок і границь; мультиевристичного алгоритму вершинної мінімізації та алгоритму генерації диз’юнктивно-нормальної форми представлення випадковими гранями дозволили отримати лише часткові рішення, які напряму залежать від вибраного ключа і не дозволяють побудувати придатну для використання модель через обмежені можливості використання обчислювальних ресурсів.

3.3 Аналіз ефективності розробленої системи

Оцінимо криптографічну стійкість розроблених криптосистем до різних атак порушника і наведено результати експериментальних досліджень статистичної безпеки за методикою NIST STS.

Для високошвидкісних надлишкових кодів кореляційний декодер менш ефективний, ніж синдромний. При зниженні відносної швидкості кодування обчислювальна ефективність синдромного декодування знижується, а при

$R = k / n < 0{,}5$ кореляційний декодер більш прийнятний для використання його супротивником як метод крипто аналізу.

Аналіз залежностей, свідчить, що застосування переставного декодера з відомим противнику відкритим ключем при $0{,}1 \le R = k/n \le 0{,}95$ і довжині використаного коду $n = 1000$ для криптоаналізу обчислювально недоцільно, крипто-кодова система захисту інформації ефективно забезпечує безпеку передавання даних у комп'ютерних системах та мережах.

Підсумкові значення та результати кращих світових криптоалгоритмів наведено в таблиці 3.10

Таблиця 3.10 - Результати експериментального тестування

Генератор	Кількість тестів, в яких тестування пройшло ≥99% послідовностей	Кількість тестів, в яких тестування пройшло ≥96% послідовностей
BBS	134 (71%)	189 (100%)
FIPS 197	126 (67%)	189 (100%)
Розроблені крипто-кодові засоби захисту інформації	132 (69%)	189 (100%)

Таким чином, аналіз отриманих результатів експериментальних досліджень показав, що за своїми властивостями запропоновані засоби не поступаються кращим світовим аналогам. Отже, практичне застосування розроблених засобів захисту інформації дозволяє отримати хороші статистичні властивості формованих послідовностей і ефективно забезпечують безпеку даних, які опрацьовують і передають.

На рисинку 3.5 наведено залежності $S_ш(n)$ при несистематичному алгоритмі кодування (n, k, d) коду над $GF(q)$ з різною відносною швидкістю коду

$R = k/n$. На рисунку 3.6 подано залежності $S_{рш}(n)$ при використанні алгебро-геометричних кодів (АГК) і кодів Ріда – Соломона (РС), де n – довжина (n, k, d) коду над $GF(q)$.

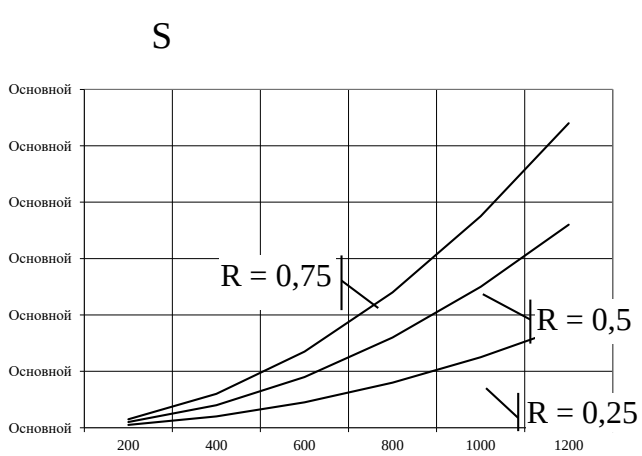


Рисунок 3.5 - Залежності складності формування криптограми

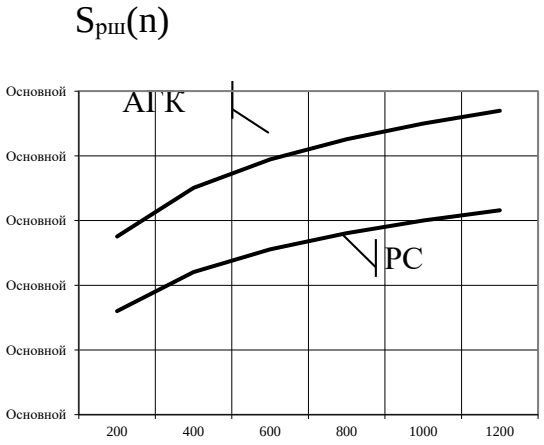


Рисунок 3.6 - Залежності складності розшифрування криптограми

Як випливає з рисунків 3.5, 3.6 крипто-кодові засоби захисту інформації мають високі показники швидкодії як при формуванні криптограми, так і при її розшифруванні. При підвищенні довжини коду складність перетворення даних росте як поліноміальна функція.

З використанням введеного узагальненого показника ефективності передавання даних в КСіМ проведено дослідження ефективності обміну даними з використанням різних криптографічних засобів захисту інформації в різних режимах управління обміном даних. Для підвищення значення показника функціональної ефективності КМ використовуються різні способи управління обміном даними: без зворотного зв’язку з виявленням r – кратних помилок; без зворотного зв’язку з виправленням t – кратних помилок; з вирішальним зворотним зв’язком і безперервним передаванням кадрів (ВЗЗбп) “Повернення–на–N”; з вирішальним зворотним зв'язком і позитивною квитанцією (ВЗЗпк). Для обліку статистичних властивостей послідовностей помилок в реальних каналах зв’язку отримано співвідношення для відповідних моделей підвищення достовірності приймання повідомлень, які передаються, в моделі каналу з

пам’яттю. Аналіз залежностей засвідчує, що найефективнішими протоколами управління обміну даними є протоколи з вирішальним зворотним зв’язком і позитивною квитанцією та з вирішальним зворотним зв'язком і безперервним передаванням кадрів “Повернення–на–N”. При використанні в протоколах обміну асиметричних криптоалгоритмів вимоги за оперативністю знижують узагальнений показник ефективності обміну даними в ГОС на 20%.

На рисунку 3.7 представлено результати досліджень ефективності передавання даних у комп’ютерних системах і мережах з використанням розроблених крипто-кодових засобів захисту інформації, симетричних і несиметричних криптосистем.

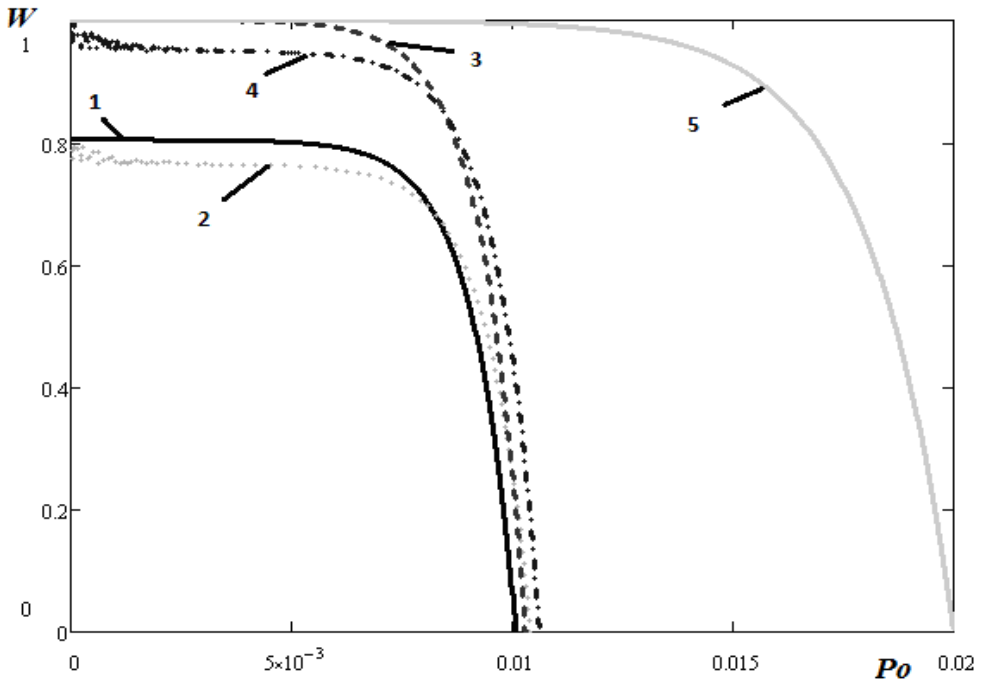


Рисунок 3.7 - Залежність показника ефективності обміну даними в комп’ютерній мережі W від ймовірності бітових помилок P_0.

Позначення графіків:

1 – “Повернення–на–N” (протокол із асиметричною криптосистемою); 2 – З ВЗЗпк асим. (з вирішальним зворотним зв’язком і позитивною квитанцією, протокол із асиметричною криптосистемою); 3 – “Повернення–на–N” (протокол

із симетричною криптосистемою); 4 – З ВЗЗпк сим. (з вирішальним зворотним зв'язком і позитивною квитанцією, протокол із симетричною криптосистемою); 5 – розроблена крипто-кодова система захисту інформації.

Аналіз рис. 23 показує, що застосування розроблених крипто-кодових систем дозволяє забезпечити необхідний показник ефективності обміну даними у комп'ютерній мережі W = 0,95 при використанні усіх видів каналів зв'язку (від дротяних ліній з $P_{пом} = 10^{-2} – 10^{-3}$ до оптоволоконних ліній з $P_{пом} = 10^{-9}–10^{-12}$).

Висновки до розділу 3

Запропонований алгоритм формування недвійкових рівновагових послідовностей реалізується через сукупність простих і обчислювально ефективних перетворень, заснованих на елементарних двійкових операціях над елементами послідовностей. З погляду практичної реалізації розробленого методу і алгоритмів недвійкового рівновагового кодування найбільш доцільним є застосування недорогих обчислювальних пристроїв на базі ПЛІС і СМАРТ-карт. Формування криптограм у запропонованих крипто-кодових засобах захисту інформації здійснюють за допомогою виконання процедур і функцій рівновагового і нерівновагового алгебраїчного кодування, методів маскування відповідних кодів під випадкову послідовність і функціональних операцій над кінцевими полями.

За результатами порівняння можна зробити висновок, що використання групи операцій додавання за модулем два з точністю перестановки на основі додаткової гамуючої послідовності забезпечить підвищення якості шифрування і надійності роботи, а при однократних відмовах каналів вхідної інформації – виключить можливість створення передумови витоку інформації чи зламу ключа.

З використанням введеного узагальненого показника ефективності передавання даних в КСіМ проведено дослідження ефективності обміну даними

з використанням різних криптографічних засобів захисту інформації в різних режимах управління обміном даних. Для підвищення значення показника функціональної ефективності КМ використовувались різні способи управління обміном даними. Аналіз показав, що застосування розроблених крипто-кодових систем дозволяє забезпечити необхідний показник ефективності обміну даними у комп'ютерній мережі W = 0,95 при використанні усіх видів каналів зв'язку (від дротяних до оптоволоконних ліній).

ВИСНОВКИ

В дипломній роботі отримано теоретичне узагальнення і розв'язання науково-технічної задачі, що полягає в розробленні методу побудови крипто-кодових засобів захисту інформації на основі недвійкових рівновагових кодів і

забезпечує підвищення безпеки і достовірності передавання даних у комп’ютерних системах і мережах.

На основі аналізу відомих методів забезпечення безпеки і достовірності обґрунтовано перспективні напрями розвитку систем захисту інформації, які дозволяють інтегрувати методи криптографічного перетворення і канального (завадостійкого) кодування даних та підвищують ефективність передавання даних у комп’ютерних системах і мережах.

Запропоновано метод формування сеансових криптографічних ключів, який реалізується з використанням розроблених процедур рівновагового недвійкового кодування і дає можливість адаптивної зміни ваги формованих послідовностей інтегровано забезпечувати необхідні показники безпеки і достовірності передавання даних в комп’ютерних системах і мережах у режимі прямого виправлення помилок.

Створено математичну модель крипто-кодової системи захисту інформації, яка враховує як особливості формування криптограм із використанням недвійкових рівновагових кодів, так і їх зворотного крипто-кодового перетворення на прийманні у режимі виявлення помилок і автоматичного перезапиту.

Вдосконалено протоколи обміну секретними повідомленнями як в режимі прямого виправлення помилок, так і в режимі виявлення помилок з автоматичним перезапитом даних, які на відміну від відомих використовують крипто-кодові засоби з недвійковими рівновагових кодами, що підвищило захищеність даних від дії випадкових помилок в каналах зв’язку, а також від цільового впливу зловмисників.

Отримано оцінки стійкості розроблених крипто-кодових засобів захисту інформації до різних атак порушника. Встановлено, що при відносній швидкості і довжині використовуваного коду криптоаналіз для зловмисника обчислювально недосяжний, складність реалізації найефективнішої атаки зловмисника складає не менше 2^{35} групових операцій над полем *GF(q)*. За своїми показниками запропоновані засоби майже не поступаються відомим криптосистемам за

методикою статистичного тестування NIST STS (зі 189 статистичних тестів 132 тести (69%) задовольняють критерію [$0.99 \leq r_j \leq 1.00$] і 189 тестів (100%) – критерію [$0.96 \leq r_j \leq 1.00$]).

Отримано оцінки складності реалізації розроблених крипто-кодових засобів захисту інформації. Розроблені крипто-кодові засоби захисту інформації дозволяють реалізувати швидке (10-100 Мбіт/с) криптографічне перетворення великих обсягів даних з використанням відкритих ключів. З точки зору практичної реалізації розробленого методу найбільш доцільним є застосування недорогих обчислювальних пристроїв на базі ПЛІС і СМАРТ-карт.

Отримані оцінки узагальненого показника ефективності розроблених крипто-кодових систем свідчать, що ці системи дають змогу збільшити узагальнений показник ефективності до рівня $W(P_{пом})_{отрим} = 0{,}95$, при цьому забезпечено його приріст на 0,05 при показнику криптостійкості $B = 10^{30} - 10^{35}$ групових операцій, $t_ш = t_{розш} = 0{,}1$с зі швидкістю $S_ш(n) = S_{розш}(n) = 10 - 100$ Мбіт/с, і ймовірністю помилки $P_{пом} = 10^{-2} – 10^{-3}$, що в повному обсязі задовольняють вимогам до сучасних КСіМ.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації:* зб. наук. / Бабенко В. Г., Лада Н. В. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116–118.

2. Бабенко В. Г., Лада Н. В., Лада С. В. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. *Вісник Черкаського державного технологічного університету*. / Бабенко В. Г., Лада Н. В., Лада С. В. 2016. № 1. С. 5–11.

3. Лада Н. В. Аналіз коректності взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації./ Лада Н. В. *Системи управління, навігації та зв'язку: Полтава : ПНТУ, 2015. - Вип. 4 (36). - С. 73-78.*

4. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. *The scientific potential of the present*: proceedings of the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. С. 108–111. (Шотландия, Логос)

5. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два./ Бабенко В. Г., Лада Н. В. - *Smart and Young*: щомісячний наук. журн. 2016. № 11–12. Ч. 1. С. 49–54.

6. Криптографическое кодирование: кол. монография / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240 с.

7. Бабенко В. Г., Лада Н. В., Лада С. В. Взаємозв'язки між операціями в матричних моделях криптографічного перетворення. *Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі*: матеріали Першої міжнар. наук.-практ. Конф / Бабенко В. Г., Лада Н. В., Лада С. В - 1 квіт. 2016 р. С. 17.

8. Бабенко В. Г., Лада Н. В. Дослідження симетричних дворозрядних двохоперандних операцій для криптоперетворення. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління*: матеріали П’ятої міжнар. наук.-техн. конф.: тези доп / Бабенко В. Г., Лада Н. В. Харків, 23–24 квіт. 2015 р. С. 59.

9. Бабенко В. Г., Лада Н. В. Дослідження множини операцій криптографічного додавання. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014)*: тези доп. ІІ міжнар. наук.-практ. конф., / Бабенко В. Г., Лада Н. В. Черкаси: ЧДТУ, 2014. Т. 1. С. 135–136.

10. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множин операцій, синтезованих на основі додавання за модулем два. *Методи та засоби кодування, захисту й ущільнення інформації*: тези доп. П’ятої міжнар. наук.-практ. конф., / Бабенко В. Г., Лада Н. В., Лада С. В. Вінниця: Нілан-ЛТД, 2016. С. 54–57.

11. Лада Н. В. Використання графічного представлення операцій для виявлення їх взаємозв’язків в моделях операцій криптографічного перетворення. *Проблеми інформатизації*: матеріали Четвертої міжнар. наук.-техн. конф.: тези доп.,/ Лада Н. В. Черкаси: ЧДТУ, 2016. С. 9–10.

12. Крипографічний захист інформації [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/ Крипографічний_захист_інформації

13. Засоби та методи захисту інформації [Електронний ресурс] –Режим доступу до ресурсу: https://buklib.net/books/28625/

14. Метод недвійкового рівно вагового кодування [Електронний ресурс] –Режим доступу до ресурсу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/957

15. Принцип шифрования гаммированием [Електронний ресурс] – Режим доступу до ресурсу: http://crypto.pp.ua/2010/04/82/

16. Криптографические средства защиты информации [Електронний ресурс] –Режим доступу до ресурсу: http://infosecmd.narod.ru/gl5.html

17. Анализ эффективности [Електронний ресурс] –Режим доступу до ресурсу: https://scienceforum.ru/2017/article/2017031562

18. Сучасний захист інформації [Електронний ресурс] –Режим доступу до ресурсу: http://journals.dut.edu.ua/index.php/dataprotect/index

19. Технології захисту інформації в інформаційних системах [Електронний ресурс] –Режим доступу до ресурсу: https://stud.com.ua/50143/informatika/tehnologiyi_zahistu_informatsiyi_informatsiynih_sistemah_kompyuternih_merezhah